Ruprecht-Karls-Universität Heidelberg
Hochschule Heilbronn

Diplomstudiengang Medizinische Informatik

Februar 2010

Diplomarbeit

Konzept und Implementierung eines Standard-basierten Webservices
zur Einwilligungserstellung für ein zentrales Einwilligungsmanagement

Lennart Köster

Referent:	Prof. Dr. Björn Bergh (Universität Heidelberg)
Korreferent:	Prof. Dr. Martin Haag (Hochschule Heilbronn)
Betreuende Assistenten:	Dipl.-Inform. Med. Oliver Heinze
	Dipl.-Inform. Med. Markus Birkle

Danksagungen

Allen voran möchte ich meinen Eltern für ihre Unterstützung während meines Studiums und für die Ermöglichung desselben danken. Ihr Rat und ihre Hilfe waren stets Motivation für mich dieses Studium zu einem erfolgreichen Abschluss zu bringen.

Danken möchte ich dem Direktor des Zentrums für Informations- und Medizintechnik des Universitätsklinikums Heidelberg Prof. Dr. Björn Bergh für die Möglichkeit dieses Thema in meiner Abschlussarbeit zu bearbeiten und für die Übernahme des Referates. Mein Dank gilt auch Prof. Dr. Martin Haag für die Übernahme des Korreferates und die Betreuung meiner vorangegangenen Studienarbeit, welche mir bei den Formalismen der Beschreibung der Implementierung dieser Arbeit sehr nützlich war.

Letztlich möchte ich meinen beiden betreuenden Assistenten Dipl.-Inform. Med. Oliver Heinze und Dipl.-Inform. Med. Markus Birkle für die sehr gute Betreuung dieser Arbeit und die vielen konstruktiven Vorschläge und Anregungen zu den Teilergebnissen derselben danken. Besonders möchte ich beiden für das Korrekturlesen dieser Arbeit danken.

Zusammenfassung

Durch die immer härteren Anforderungen an Wirtschaftlichkeit und Qualität ihrer angebotenen Leistungen kommt es in der Medizin zur immer engeren Zusammenarbeit zwischen den Leistungserbringern. Das Universitätsklinikum Heidelberg und die IntercomponentWare AG haben daher ein gemeinsames Projekt ins Leben gerufen dessen Ziel die Entwicklung eines intersektoralen Informationssystems (ISIS) ist. ISIS soll den Austausch versorgungsrelevanter, medizinischer Daten ermöglichen.
Patienten müssen der Teilnahme an ISIS und dem Austausch sowie der Verarbeitung ihrer Daten mit den einzelnen an ISIS teilnehmenden Einrichtungen aufgrund der rechtlichen Gegebenheiten in Deutschland explizit zustimmen.
Das Management der Einwilligungserklärungen wurde bisher durch Produkte der Industrie nicht zufrieden stellend gelöst. Um das Einwilligungsmanagement befriedigend zu lösen wurde am Universitätsklinikum Heidelberg ein Konzept für ein zentrales Einwilligungsmanagement für ISIS entwickelt.

Es sollte in dieser Arbeit ein System zur Erstellung von Einwilligungserklärung erstellt werden, das Teil des zentralen Konzeptes ist. Zu Beginn wurde die Leitung des ISIS Projektes im Hinblick auf ihre Vorgaben bezüglich der Verwendung etablierter Standards und Technologien befragt. Durch die Befragung wurden auch die Anforderungen an das System festgestellt. Ausgehend von den Anforderungen wurde ein Konzept für die Speicherung der Einwilligungserklärungen der Patienten in einer menschen- und maschinenlesbaren Form entwickelt. Basierend auf der Anforderungsanalyse wurden die zu verwendenden Technologien der Implementierung gewählt. Durch Analyse der rechtlichen Texte und Literatur wurde die Möglichkeit der elektronischen Signatur der Einwilligungserklärungen aufgearbeitet. Abschließend wurde das System implementiert.
Als Format für die Speicherung der Einwilligungserklärungen wurde das Basic Patient Privacy Consent IHE-Profil gewählt und an die festgestellten Anforderungen angepasst. Die Analyse der Thematik der elektronischen Signatur ergab, dass die Nutzung dieser Technologie als Alternative zur rechtskräftigen Unterschrift der Einwilligungserklärung möglich ist. Die Implementierung des Verfahrens der elektronischen Signatur wurde entsprechend umgesetzt. Die in der Anforderungsanalyse festgestellten geforderten Funktionalitäten wurden Standard-basiert implementiert.
Durch die Implementierung der geforderten Funktionalitäten wurde es ermöglicht, personalisierte Einwilligungserklärungen elektronisch zu erzeugen und zu speichern. Die Einwilligungserklärungen können mit einer elektronischen Signatur versehen werden, wodurch sie rechtliche Gültigkeit besitzen. Die implementierten Funktionen ermöglichen die Verwaltung der Benutzerschaft des implementierten Systems. Das System selbst wurde modular und Standard-basiert implementiert, um Interoperabilität zu gewährleisten.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Gegenstand und Motivation

Im Rahmen der immer härteren Anforderungen an Qualität und Wirtschaftlichkeit in der medizinischen Versorgung zeichnet sich ab, dass es zu einer erhöhten Zusammenarbeit der verschiedenen Leistungserbringer im Gesundheitswesen kommen wird. In Folge dessen wird der Datenaustausch zwischen den einzelnen Einrichtungen vermehrt in den Fokus geraten und eine wichtige Rolle spielen ([Heinze et al. 2008a]). Das Universitätsklinikum Heidelberg (UKHD) und die InterComponentWare AG (ICW) haben im Zuge dieser Entwicklung das Konzept des intersektoralen Informationssystems (ISIS) entwickelt. ISIS erlaubt es den verschiedenen teilnehmenden Einrichtungen Patientendaten untereinander auszutauschen und so die Qualität der Versorgung zu verbessern. Ziele von ISIS sind dabei unter anderem die Vermeidung von Medienbrüchen, die schnelle Übermittlung von Informationen und die Vermeidung des Verlustes von wichtigen Informationen. Besonderen Wert wurde dabei auf Standard-basierte Lösungen gelegt, um Kompatibilität und Interoperabilität zu gewährleisten. Um dies zu erreichen, werden Standards, wie zum Beispiel Health Level 7 (HL7)[1], oder Profile von Standardisierungsinitiativen, wie Integrating the Healthcare Enterprise (IHE)[2], verwendet. Der Ausbau des Projektes erfolgt dabei stufenweise. In den initialen Ausbaustufen 1 und 2 ist ISIS eine einrichtungsübergreifende elektronische Patientenakte (eEPA). Im Anschluss erfolgt der Ausbau zu Stufe 3, in der durch Integration einer elektronischen Gesundheitsakte (EGA) in ISIS das Projekt zu einer persönlichen einrichtungsübergreifenden elektronischen Patientenakte (PEPA) erweitert wird ([Heinze et al. 2008a]).

Generell ist für den Austausch von Patientendaten die Zustimmung des Patienten notwendig. Er muss der Übertragung der Daten an ISIS und dem Zugriff auf dieselben zustimmen. Erst dann können die Daten von berechtigten Personen der teilnehmenden Krankenhäuser und Arztpraxen eingesehen werden. Der Datenaustausch unterliegt dabei den datenschutzrechtlichen Bestimmungen, die der Gesetzgeber zum Schutz des Patienten aufgestellt hat. Die Einhaltung dieser Bestimmungen ist für ISIS zwingend notwendig und wird dementsprechend beachtet. In der momentanen Form des Ausbaus kann der Patient der Teilnahme an ISIS nur auf Einrichtungsebene zustimmen. Eine feinere Zustimmung auf Personen- oder Dokumentenebene ist nicht möglich. Ein weiterer Nachteil des aktuellen Ausbaus ist, dass der Patient in jeder teilnehmenden Einrichtung einwilligen muss. Dies entspricht einem dezentralen Einwilligungsmanagement.

[1] *http://www.hl7.org/*
[2] *http://www.ihe.net/*

Um das Einwilligungsmanagement zu verbessern, analysierte M. Birkle in [Birkle 2009a] die verschiedenen Möglichkeiten zur Umsetzung eines elektronischen Einwilligungsmanagements für die Einwilligungen der Patienten zur Teilnahme an ISIS. Die im Rahmen des ISIS Projektes favorisierte Lösung für die Problematik des Einwilligungsmanagements beruht dabei auf einer zentralen elektronischen Verwaltung der Einwilligungserklärungen. Patienten, die an ISIS teilnehmen möchten, geben ihren Willen und ihre Vorgaben zum Datenaustausch mit der jeweiligen Einrichtung an das aufklärende Einrichtungspersonal weiter. Das Einrichtungspersonal erstellt daraufhin eine papierbasierte Einwilligungserklärung, in welcher der Patient der Teilnahme an ISIS zustimmt und welche die Datenverarbeitung der an der Einrichtung anfallenden Daten für ISIS ermöglicht. Sobald ISIS sich zu einer PEPA entwickelt hat, wird es den Patienten selbst möglich sein, ihre Einwilligungseinstellungen gemäß ihrer Vorgaben anzupassen ([Heinze et al. 2008b]). Im Zuge dieser Entwicklung sollen die Einwilligungserklärungen der Patienten elektronisch in einem Consent Manager (Siehe Glossar - Anhang A) gespeichert werden. Die Erstellung der Einwilligungserklärungen soll dann ebenfalls elektronisch über ein entsprechendes System erfolgen. Die Entwicklung dieses Systems ist Gegenstand dieser Arbeit.

1.2 Problemstellung

Das benötigte System zur Erstellung der Einwilligungserklärungen, im weiteren Consent Creator, wurde bisher nicht implementiert. Der Consent Creator muss dabei, um semantische Interoperabilität zu gewährleisten, gemäß Standards implementiert werden. Die Frage nach dem Format für die Speicherung der Einwilligungserklärungen ist unbeantwortet. Es gibt bisher kein Standard-basiertes Format für die Speicherung einer elektronischen Einwilligungserklärung. Die elektronischen Einwilligungserklärungen müssen gemäß der Wünsche der Patienten dynamisch erzeugt werden. Um eine Einwilligung, die rechtlich verbindlich ist, zu erhalten, muss sie bisher ausgedruckt und vom Patienten eigenhändig unterschrieben werden. Eine Möglichkeit, die Einwilligungserklärung elektronisch rechtssicher zu speichern wurde bisher nicht gefunden. Die Implementierung einer elektronischen Signatur könnte die rechtssichere Speicherung ermöglichen und es Patienten ermöglichen auch von zuhause Änderungen an ihrer Einwilligungserklärung vorzunehmen. Entsprechende technische Rahmenbedingungen sind bisher jedoch nicht aufgearbeitet worden. Die elektronischen Einwilligungserklärungen müssen von allen an ISIS teilnehmenden Einrichtungen aus erzeugt werden können.

1.3 Zielsetzung

Im Rahmen dieser Diplomarbeit soll nun der in der Problemstellung angesprochene Consent Creator implementiert werden.
Aus der bereits dargelegten Problemstellung lassen sich folgende Ziele ableiten:

1. Es soll zentraler Service für die Erzeugung der Datenschutzregeln und Einwilligungserklärungen der Patienten implementiert werden, der sich in das in [Birkle 2009a] definierte zentrale Konzept für ein Einwilligungsmanagement eingliedert und folgende Funktionalitäten bietet:

   a) Möglichkeit der Erstellung von Einwilligungserklärungen.

   b) Modularer Aufbau mit Standard-basierten Schnittstellen für die Interaktion mit anderen Systemen.

   c) Interoperabilität.

2. Die Einwilligungserklärungen müssen folgende Punkte berücksichtigen:

   a) Es soll eine Struktur für die Einwilligungserklärungen der Patienten erarbeitet werden.

   b) Es soll eine optimale Lösung für das Format der Datenschutzregeln sowie deren Überführung in eine menschenlesbare Einwilligungserklärung gefunden werden.

4. Es sollen die technischen Rahmenbedigungen für die Implementierung einer elektronischen Signatur in den Service erarbeitet werden.

5. Der Service sollte es ermöglichen Einwilligungserklärungen mit einer elektronischen Signatur zu versehen.

1.4 Aufgabenstellung

Aus den in Abschnitt 1.3 genannten Zielen leiten sich folgende Aufgabenstellungen ab:

1. Erarbeitung einer Lösung für die elektronische Erstellung einer Einwilligungserklärung

2. Erarbeitung einer Struktur für eine elektronische Einwilligungserklärung.

3. Erarbeitung einer Lösung für das Format der Datenschutzregeln und deren Transformation zu einer Einwilligungserklärung.

4. Erarbeitung der technischen Rahmenbedigungen für eine elektronische Signatur der Einwilligungserklärungen sowie Implementierung.

1.5 Aufbau der Diplomarbeit

Die vorliegende Arbeit gliedert sich in sieben Kapitel. Die Arbeit gibt zunächst in Kapitel 2 einen Einblick in den Aufbau des intersektoralen Informationsformationssystems. Anschließend werden die für die Arbeit wichtigen Datenschutzgesetze dargelegt, welche die Verarbeitung von Patientendaten und die Einwilligungserklärung des Patienten betreffen. Darüber hinaus sind für diese Arbeit wichtige Standards und Standardisierungsinitiativen sowie das Thema elektronische Signatur teil des Grundlagenkapitels. Ein Überblick über die bisherigen Lösungsansätze zur Erstellung von Einwilligungserklärungen schliesst dieses Kapitel ab.

Kapitel 3 beschreibt die verwendeten Methoden und Werkzeuge dieser Arbeit.

Kapitel 4 legt die Ergebnisse der Anforderungsanalyse dar. Anforderungen wurden für die Teilgebiete Funktionalität des Consent Creators, die Einwilligungserklärung der Patienten und den Webservice definiert.

Das entwickelte Konzept zur elektronischen Speicherung der Einwilligungserklärungen wird in Kapitel 5 dargestellt.

In Kapitel 6 wird die Implementierung des Webservices veranschaulicht. Die Oberfläche mit der verbundenen Funktionalität wird erklärt, es wird die Implementierung des Servers und der Aufbau des Datenbankschemas beschrieben.

Kapitel 7 befasst sich mit dem Test der in Kapitel 5 beschriebenen Implementierung, teile dieses Kapitels sind sowohl die formalen Tests der Implementierung sowie die Tests der Oberfläche.

Diskussion und Ausblick der Arbeit befinden sich schließlich in Kapitel 8.

2 Grundlagen

Basierend auf den vorangegangenen Erläuterungen zur Problemstellung, den zu erreichenden Zielen und damit verbundenen Aufgaben sowie zum Aufbau der Arbeit soll in diesem Kapitel das Basiswissen für das Verständnis der Arbeit und des entwickleten Architekturentwurfs mit dem darin enthaltenen Konzept gelegt werden. Hierfür ist es nötig zu verstehen, wie die jeweiligen verwendeten Technologien funktionieren und einbezogenen Standards strukturiert sind. Zudem soll erläutert werden, welche Ziele mit ISIS verfolgt werden und wie das intersektorale Informationssystem aufgebaut ist.

2.1 Intersektorales Informationssystem (ISIS)

Das intersektorale Informationssystem (ISIS) ist ein gemeinschaftliches Projekt des Uniklinikums Heidelberg (UKHD) und der IntercomponentWare AG (ICW) Walldorf, welches das Ziel hat, den reibungslosen Datenaustausch zwischen kooperierenden Krankenhäusern und Arztpraxen zu ermöglichen ([Heinze et al. 2008c]). Die Entwicklung von ISIS ist dem Trend zur integrierten Versorgnung geschuldet. Patienten werden nicht mehr nur von einer Organisation behandelt, sondern gezielt von mehreren Organisationen versorgt. Dies bedingt den Informationsfluss über mehrere Organisationen hinweg, um zum Beispiel mehrfache Untersuchungen zu vermeiden. Einzelne Organisationen führen bisher elektronische Patientenakten (EPA). Diese Akten enthalten patientenbezogene, medizinische und medizinisch relevante Informationen eines Patienten die an genau einer Einrichtung angefallen sind ([Schmücker et al. 1998]). Diese Akten sind in den Organisationen in Systemen gespeichert, die es nicht ermöglichen Daten gezielt mit anderen Organisationen auszutauschen ([Heinze et al. 2008b]). Es ist daher nötig die EPA zu einer einrichtungsübergreifenden elektronischen Patientenakte (eEPA) zu erweitern und diese allen an der Behandlung Beteiligten zur Verfügung zu stellen. Eine eEPA stellt die gesammelten, medizinisch relevanten Informationen eines Patienten institutionsübergreifend auf digitalen Datenträgern allen an der Behandlung Beteiligten zur Verfügung ([Brenner 2001]). Zusätzlich zu dieser Entwicklung gilt es auch den Patienten stärker zu berücksichtigen. Mit diesem Ziel wurde die elektronische Gesundheitsakte (EGA) entwickelt. Eine EGA ist, im Gegensatz zu den arztmoderierten Akten EPA und eEPA, patientenmoderiert und ermöglicht es dem Patienten selbst Informationen in die Akte einzustellen ([Warda 2005]). Die EGA soll es dem Patienten ermöglichen selbst Einsicht in seine Akte zu nehmen und Inhalte, wie Daten über chronische Erkrankungen, hinzuzufügen ([Heinze et al. 2008c]). ISIS versucht diesen Entwicklungen Rechnung zu tragen und Erfahrungen beim Aufbau dieser Aktengeneration zu sammeln und praktikable Lösungen für auftretende Probleme zu entwickeln. Die bisher aufgetretenen Probleme waren weniger technischer denn datenschutzrechtlicher Natur ([Heinze et al. 2008a]).

Der Ausbau von ISIS erfolgt stufenweise, Stufe 1 hat den Aufbau einer eEPA zwischen dem UKHD und vier weiteren Kliniken der Gesundheitszentren Rhein-Neckar gGmbH zum Ziel. In Stufe 2 werden zusätzlich Arztpraxen aus der Region an die eEPA angeschlossen. Stufe 3 hat schlussendlich den Aufbau einer EGA, und die Integration derselben in die eEPA, zum Ziel. Das Ergebnis ist dann eine persönliche, einrichtungsübergreifende, elektronische Patientenakte (PEPA). Um Daten zwischen den teilnehmenden Organisationen auszutauschen ist es nötig, Patienten gezielt und korrekt identifizieren zu können. Hierfür kommt der Master Patient Index (MPI) des Produktes Professional Exchange Server (PXS) der ICW zum Einsatz ([Heinze et al. 2008c]).

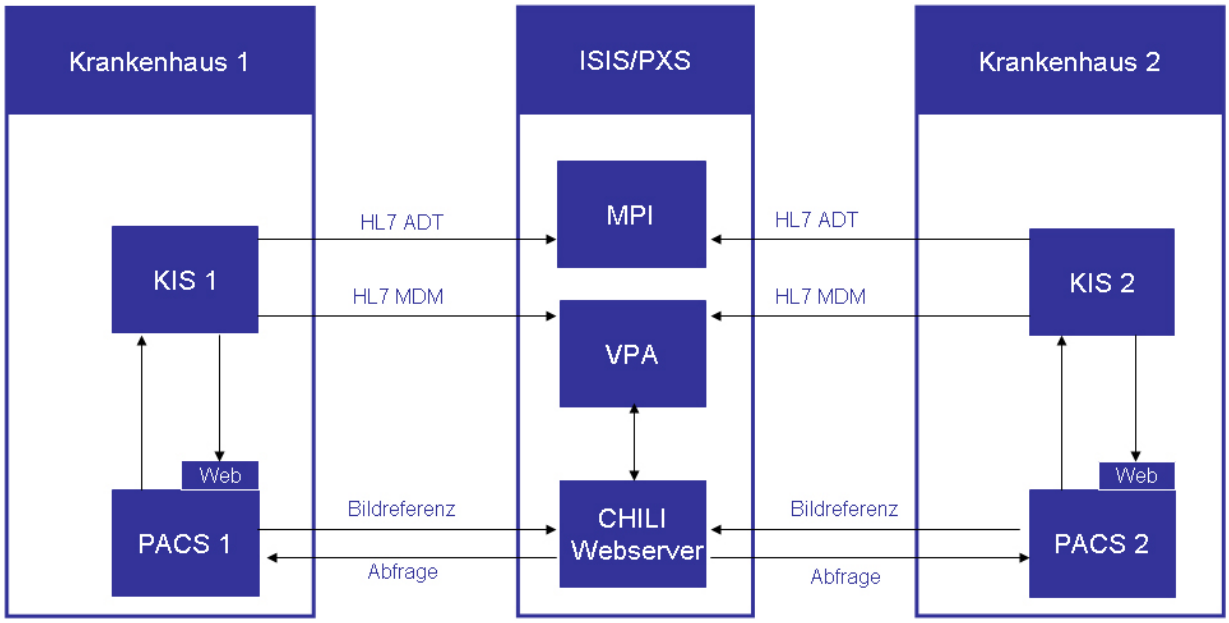

Abbildung 1: ISIS und ICW PXS [Heinze et al. 2008c]

PXS, siehe Abbildung 1, ermöglicht es, Daten aus lokalen Informationssystemen gesamtheitlich zu betrachten ([ICW 2009a]). Dies wird zum einen durch den MPI ermöglicht, welcher jedem Patienten einen eindeutigen Identifikator für PXS zuweist und diesen Identifikator mit den Identfikatoren der lokalen Systeme verknüpft ([ICW 2009b]) Der Patient besitzt daher neben der Patienten-IDs, welche jedes lokale System lokal als eindeutige Referenz benutzt, auch eine MPI-ID mit der er innerhalb der ISIS Teilsysteme identifiziert werden kann. Die lokalen Systeme erfassen die Stammdaten eines Patienten und gleichen diese mit dem MPI ab, werden genügend Übereinstimmungen bei einem Merksmalsabgleich erkannt, so wird die Patienten-ID des lokalen Systems der ID des Referenzpatienten im MPI zugeordnet [Heinze et al. 2008c]. Sollten nicht genügend Übereinstimmungen der

Mermalskriterien erfüllt sein, wird der Datensatz an eine manuelle Überprüfung weitergegeben. Daten aus den lokalen Systemen werden in der virtuellen Patientenakte (VPA) gespeichert und können von berechtigten Personen eingesehen werden. Die Daten in den Primärsystemen bleiben dabei erhalten. Im PXS werden die Daten redundant vorgehalten. Die Integration der Primärsysteme erfolgt über den Medizinischen Service Bus (MSB), welcher etablierte Standards, wie etwa HL7 oder IHE, unterstützt, jedoch auch auf individuelle Anforderungen angepasst werden kann. Neben den standardkonformen Schnittstellen bietet PXS unter anderem den Vorteil, webbasiert und somit plattformunabhängig zu sein ([ICW 2009a]). Der Austausch von Daten über den MSB erfolgt dabei mittels HL7. Bilddaten werden, aufgrund des Datenvolumens, nur in den Primärsystemen vorgehalten und von dort mittels Digital Imaging and Communications in Medicine (DICOM)[3] abgefragt ([Heinze et al. 2008c]).
Daten werden nur nach der Zustimmung des Patienten, gemäß dem Opt-In Verfahren (Siehe Glossar - Anhang A), an ISIS übermittelt, ebenso werden geltende Datenschutzgesetze umfassend berücksichtigt. Der Zugriff auf Informationen, welche in ISIS gespeichert sind, erfolgt nur nach vorhergehender Authentifizierung des externen Client, darüberhinaus wird die Verbindung durch einen VPN-Tunnel geschützt.
Informationen über Organisationen, die an ISIS teilnehmen, werden mittels des Provider and Organization Registry Service ([Heinze et al. 2010]) verwaltet. Organisationen und Ärzte besitzen im deutschen Gesundheitssystem eine eindeutige Identifikationsnummer, die Betriebsstättennummer und die lebenslange Arztnummer. Ein Arzt kann jedoch mehrere Arztnummern haben, beispielsweise wenn er mehreren Fachgruppen angehört. Mittels dieser Identifikationsnummer werden Organisationen und Ärzte in PORS registriert. Anschließend ist es möglich, für interagierende Services, Informationen über die Organisationen abzufragen, ähnlich der gelben Seiten ([PORS]).
Ziel von ISIS ist es, Informationen über gemeinsame Patienten verschiedener Organisationen ohne Medienbrüche einrichtungsübergreifend auszutauschen. ISIS soll dabei, mittels einer webbasierten Plattform, eine einheitliche Sicht auf die medizinische Dokumentation des Patienten bieten, ohne bereits existierende Primärsysteme zu ersetzen. Der Zugriff für den Patienten soll dabei mit der aktuellen Telematikstruktur kompatibel sein, um ihm selbst den Zugriff auf seine Daten zu ermöglichen und sein Recht auf informationelle Selbstbestimmung umzusetzen. ISIS hat deshalb zum Ziel den Patienten als alleinigen Besitzer seiner medizinischen Daten in den Mittelpunkt zu stellen ([Heinze et al. 2008c]).

[3] http://medical.nema.org/

2.2 Datenschutzregeln

Die Daten eines jeden Patienten unterliegen gesetzlichen Rahmenbedingungen, welche die Weitergabe und Verarbeitung der Daten explizit regeln. Ebenso unterliegt die Beziehung zwischen dem Personal der Leistungserbringer und dem Patienten gesetzlichen Bestimmungen.
Zwischen Patienten und dem behandelnden Arzt existiert das Privatgeheimnis, festgehalten in § 203 Nr. 1 Strafgesetzbuch (StGB, [Bund 2010a]). Dieses verpflichtet den behandelnden Arzt über alles, was dem Arzt durch den Patienten anvertraut wurde, zu schweigen. Ebenso unterliegen andere an der Behandlung beteiligte Personengruppe dieser Geheimhaltungspflicht (§203 Nr.3 bis Nr. 6 StGB).
Die Daten der Patienten unterliegen dabei einer Vielzahl von Gesetzen, neben dem §203 Strafgesetzbuch auch § 1 Nr. 1 und Nr. 2 des Bundesdatenschutzgesetz (BDSG, [Bund 2009a]) und § 43 des Landeskrankenhausgesetz Baden-Württemberg (LKHG BW, [Land 2007]). Daten dürfen verarbeitet werden, wenn dies für die Versorgung des Patienten, deren Dokumentation und für die *„verwaltungsmäßige Abwicklung des Behandlungsverhältnisses“* erforderlich ist (§45 Nr. 1 LKHG BW). §45 Nr. 3 LKHG BW ermöglicht zudem auch die Verarbeitung zum Zwecke der Qualitätssicherung in der stationären Versorgung, zur Rechnungsprüfung und zur *„Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung“* (§45 Nr. 3 LKHG BW), wenn diese Ziele nicht mit anonymisierten Daten erreicht werden können.
Ebenso wie die Verarbeitung unterliegt auch die Übermittlung der Daten eines Patienten Beschränkungen. §46 Nr. 1 des LKHG BW erlaubt unter anderem die Übermittlung zum Zwecke der Durchführung von medizinischen Forschungsvorhaben, im Falle eines Rechttstreits, in dem die Daten benötigt werden, und bei Gefahr im Verzug. Eingeschränkt werden diese Gründe durch den Zusatz, dass die Übermittlung nur zulässig ist, wenn die Zwecke nicht mit anonymisierten Daten erreicht werden können. Zusätzlich lockert §46 Nr. 2 LKHG BW den bereits genannten §203 StGB dahingehend, dass *„Patientendaten, die der Geheimhaltungspflicht im Sinne von § 203 StGB unterliegen, auch dann übermittelt werden dürfen, wenn das Patientengeheimnis nach dieser Vorschrift nicht unbefugt offenbart würde“* (§46 Nr. 2 LKHG BW).
Vor diesem Hintergrund ist es für alle Formen der Datenverarbeitung nötig, welche nicht von den bereits genannten Gesetzen zugelassen werden, eine Einwilligung des Patienten einzuholen (§50 Nr. 1 LKHG BW). Der Patient ist über die Folgen seiner Einwilligung aufzuklären, insbesondere den Zweck der Erhebung, Verarbeitung und Nutzung der erhobenen Daten. Zusätzlich muss der Patient darauf hingewiesen werden, welche Folgen es für ihn hat, sollte er keine Einwilligung erteilen. Dem Patienten muss es auch möglich sein, seine Einwilligung jederzeit zu widerrufen. Die Einwilligung ist nur gültig, so sie auf der freien Entscheidung des Patienten beruht (§4a Nr. 1 BDSG).

Im Umkehrschluss ist es jedoch nicht möglich, dem Patienten eine pauschale Einwilligung abzuverlangen, um jetztige und später mögliche Datenverarbeitung verbindlich zu vereinbaren. Die Tragweite einer Einwilligungserklärung muss für den Patienten ersichtlich sein ([Meier 2003 S,80]). Daten von denen der Patient keine Kenntis hat, können nicht von einer Einwilligung abgedeckt werden. In einem solchen Fall muss der Patient explizit darüber informiert werden, welche seiner Daten von der Einwilligung betroffen sind ([Meier 2003 S,81]). Die Aufklärung über die Folgen und Risiken seines Handelns bedingen den sogenannten „Informed Consent“, die aufgeklärte Einwilligung.
Grundsätzlich sind Einwilligungen im deutschen Gesundheitssystem als Opt-In Einwilligungen zu verstehen. Dies bedeutet, dass der Patient der Behandlung und Datenverarbeitung zustimmen explizit zustimmen muss, wenn dies nicht bereits gesetzlich geregelt ist. Andernfalls sind die getroffenen Maßnahmen rechtswidrig ([Ärzteblatt 2007]).
Auf der anderen Seite steht das Opt-Out System. In diesem System wird die Einwilligung eines jeden Patienten implizit angenommen, ohne dies mit dem Patienten explizit abgesprochen zu haben. Der Patient kann seine Einwilligung jedoch zurücknehmen und aus dem System aussteigen, beispielsweise aus der standardisierten Verarbeitung seiner Daten ([Tuffs 2007]).

2.3 Standard- und Profilinitiativen

[ISO 2004] definiert einen Standard als *„Dokument, etabliert durch Konsens und abgesegnet durch eine anerkannte Autorität, das, für allgemeinen und wiederholten Nutzen, Regeln, Richtlinien oder Charakteristika für Aktivitäten oder ihre Resultate zur Verfügung stellt, mit dem Ziel den optimalen Grad an Ordnung in einem gegebenen Kontext zu erreichen“.*
Ein Standard kann helfen Ordnung in einen Bereich zu bringen, der bisher durch keine oder heterogene Lösungen gekennzeichnet war, die unabhängig voneinander entwickelt wurden und möglicherweise nicht miteinander kompatibel sind. Die durch Konsens etablierte Vorgehensweise ermöglicht es neuen Anwendern schnell und verständlich Lösungen umzusetzen, ohne dabei das Rad neu erfinden zu müssen. Im selben Zug erhalten die Benutzergruppen, welche den Standard umsetzen, die Möglichkeit der Vergleichbarkeit und Interoperabilität. Gerade die Erarbeitung eines Standards durch Konsens ist durch die Anzahl der Teilnehmer am Konsens und ihr gesammeltes Wissen, sowie ihre Erfahrung, nicht von einer einzelnen Gruppe, die ihre eigene Lösung sucht, aufzuwiegen ([COPRAS 2007]).
Standards spielen daher eine immer wichtigere Rolle, gerade im Bereich der Medizinischen Informatik, wo heterogene Systemlandschaften aufgrund der Vielzahl der benötigten Funktionalitäten keine Ausnahme bilden. Als Beispiel für etablierte Standards seien an dieser Stelle Health Level 7 (HL7) für einen Kommunikationsstandard mit weiter Verbreitung und HL7 Clinical Document Architecture als Dokumentenstandard für den Austausch von

Dokumenten zwischen Organisationen genannt.
Der HL7 Kommunikationsstandard wird dabei von einer eigenen Anwendergruppe entwickelt. Die Entwicklung von Standards wird in der Regel von Standardisierungsorganisationen vorangetrieben, welche auf nationaler oder internationaler Ebene veröffentlichen. Die International Organisation for Standardization (ISO) ist nach eigenen Angaben die größte Organisation, die Standards entwickelt. Entwickelt werden dabei Standards basierend auf den Vorgaben ihrer Mitglieder, unter anderem im Bereich der Medizin. Die Vorgaben werden von der Organisation aufgenommen und dann an das entsprechende Kommitee, welches Standards in diesem Bereich entwickelt, weiter geleitet. ISO verfügt zum Erstellungszeitpunkt dieser Diplomarbeit über mehr als 16.000 Standards und besitzt ein Netzwerk von 163 nationalen Instituten ([ISO 2010]).
Zusätzlich zu Standards gibt es Profilinitiativen, die versuchen dem Entwickler durch das Bereitstellen definierter Profile Lösungen aufzuzeigen. Integrating the Healthcare Enterprise bespielsweise bietet Profile für den Datenaustausch von Gesundheitsdokumenten zwischen Einrichtungen des Gesundheitswesens. Diese Profile stellen dem Entwickler Anwendungsfälle, benötigte Teilkomponenten und Transaktionen zwischen den Komponenten zur Verfügung, um ihm eine Möglichkeit für die standardgemäße Implementierung eines Standards zu bieten und mit diesem effiziente Interoperabilität zu erreichen ([IHE 2010a]). Profilinitiativen basieren dabei auf etablierten Standards und nutzen diese um Probleme zu lösen.

2.3.1 Extensible Markup Language (XML)

Die eXtensible Markup Language (XML) ist ein W3C-Standard[4] für Markup (siehe Anhang A - Glossar) in Dokumenten. XML gibt eine Syntax vor, mit der Daten, in einfachen Elementen, menschenlesbar dargestellt werden können ([XML 2004]). XML ist eine Weiterentwicklung der Standard Generalized Markup Language (SGML). SGML wurde mit dem Ziel entwickelt, es zu ermöglichen, SGML ähnlich HTML zu versenden, darzustellen und zu verarbeiten. XML wurde unter der Schirmherrschaft der W3C von der XML Working Group entwickelt und sollte ein Applikationsprofil oder eine restriktivere Form von SGML werden, jedoch weiterhin SGML konform sein. Ziele bei der Entwicklung von XML sind unter anderem die Nutzung über das Internet, Interoperabilität, Konformität mit SGML, einfache Nutzung, restriktive Handhabung, sowie Lesbarkeit für Menschen und schnelle Bereitstellung. Des Weiteren sollte das XML Design formal und präzise sein ([XML 2008] 1.1).
XML Dokumente sind aus Speichereinheiten, welche Entitäten genannt werden, aufgebaut. Diese Entitäten enthalten strukturierte oder unstrukturierte Daten. Daten werden in XML entweder durch Text oder durch Markup dargestellt. Markup beschreibt die logische und

[4] *http://www.w3.org/*

Speicherstruktur eines Dokuments, XML bietet Mechanismen um beide zu beschränken. Markup baut dabei auf mehreren Bausteinen auf:

◇ **Deklarationen** - Sie beinhalten grundlegende Informationen, welche das XML Dokument als solches identifizieren. Sie beinhalten Informationen über die XML Version, den verwendeten Zeichensatz und ob es zusätzliche Dokumente, die für die Verarbeitung notwendig sind, gibt.
<?xml version=”version_number”
encoding=”encoding_declaration” standalone=”standalone_status” ?>.

◇ **Elemente** - Sie enthalten Daten zwischen zwei sogenannten Tags, welche das Element einleiten und beenden, <tag>Inhalt</tag>. Elemente bilden die grundlegenden Einheiten eines XML Dokumentes.

◇ **Attribute** - Sie ermöglichen es einem Elemente eine deskriptive Beschreibung anzufügen und können einem Element mehrfach zugewiesen werden. Das folgende Beispiel erweitert das Element <tag> um ein Attribut,
<tag attribute=”attributevalue”>Inhalt</tag>.

```
<?xml version="1.0" encoding="UTF-8" ?>
<patient>
        <patientName>
                <first>Bartholomew</first>
                <last>Simpson</last>
        </patientName>
        <patientContact>
                <street>27 Shelbyville Road</street>
                <city>Springfield</city>
                <state>MA</state>
                <zip>12345</zip>
                <phone>555.123.4567</phone>
                <fax/>
                <email/>
        </patientContact>
        <patientDoB>1992-03-21</patientDoB>
        <patientGender>male</patientGender>
        <patient-number>555555</patient-number>
</patient>
```

Abbildung 2: Beispiel XML Markup

Der Aufbau der Elemente folgt dabei dem Prinzip einer Baumstruktur. In dieser Struktur können sich Elemente immer weiter verzweigen in dem sie in sich weitere Elemente beinhalten. Abbildung 2 illustriert dies beispielhaft. Der große Vorteil von XML ist die

Flexibilität mit welcher das Markup angepasst und erweitert werden kann, um den eigenen Anforderungen zu genügen. So können eigene Tags definiert werden, mit denen sich alle benötigten Informationen eines thematischen Teilbereichs erfassen lassen. XML beschreibt durch die Syntax exakt welchen Anforderungen das Markup genügen muss. Unter anderem beschreibt es, wie Elemente innerhalb anderer Elemente existieren können, wie die Struktur der Tags der Elemente aufgebaut ist und welche Namen für Tags akzeptabel sind. Dokumente, welche alle Forderungen des XML Syntax bezüglich des Markups umsetzen, sind wohlgeformt und können von einem Parser maschinell verarbeitet werden. Durch die Verarbeitung durch einen Parser ist es möglich gezielt XML Dokumente weiter zu verarbeiten und in anderen Formen zu speichern, zu versenden oder zu präsentieren. XML macht über die Syntax der Dokumente hinaus keine Aussagen zur Präsentation. Es ist eine reine Auszeichnungssprache ([XML 2004]).
Neben der Wohlgeformtheit eines XML Dokuments lassen sich auch Aussagen darüber machen, ob ein Dokument vailde ist. Dazu lässt sich die sogenannte Document Type Definition (DTD) nutzen, welche ein Schema für XML Dokumente spezifiziert. Das Schema beschreibt die erwartete Struktur des Dokumentes. Der Parser kann durch DTD prüfen, ob das Dokument das DTD-Schema einhält oder nicht. Dies ist nützlich, da Wohlgeformtheit nicht hinreichend für Vailidität ist. Wohlgeformtes und valides XML lässt sich durch Transformationssprachen in andere Strukturen und Darstellungen umwandeln ([XML 2004]).

2.3.2 Extensible Stylesheet Language Transformations (XSLT)

Extensible Stylesheet Language Transformations (XSLT) ist eine deklarative auf XML basierende Sprache, um XML Dokumente in andere XML Dokumente oder Präsentationsformen zu transformieren ([XSLT 2007]). XSLT wurde als Nachfolger der Document Style Semantics and Specification Language entwickelt, einer Sprache für die Definition von SGML Transformationen ([XSLT 2008]). Wie XML wird XSLT vom W3C betreut. Der Begriff Stylesheet ist auf die Möglichkeit, mit XSLT Präsentationsinformationen für ein XML Dokument bereitzustellen, zurückzuführen. Dies geschieht durch Transformation eines XML Dokumentes in ein Dokument aus XSL formatierten Objekten. XSLT Transformationen erlauben es, Quellbäume in neue Bäume zu transformieren. Dies geschieht durch die Anwendung von Dokumentenvorlagen, in welchen Muster für die Elemente des Dokumentes gespeichert sind, sowie durch die Anwendung eines Sequenzkonstruktors auf die Muster. Durch diese Anwendung lassen sich aus dem bisherigen Quellbaum neue Bäume erstellen, welche vom bisherigen Baum komplett abweichen und Informationen auf komplett andere Art und Weise darstellen können. Die Orientierung an Elementen der XML Struktur erlaubt es XSLT Stylesheets auch auf mehrere Dokumente, welche ähnliche Strukturen haben, anzuwenden ([XSLT 2007]). XSLT kann beispielsweise zur Transforma-

tion von, auf XML basierenden, HL7 CDA Dokumenten (Siehe Abschnitt 2.3.4) in eine HTML-Darstellung genutzt werden.

2.3.3 Health Level Seven (HL7)

Health Level Seven (HL7) ist ein Standard zum Datenaustausch in einer gesundheitsbezogenen Umgebung, welcher von einer gleichnamigen Organisation seinen Mitgliedern zur Verfügung gestellt wird ([HL7 2010a]). HL7 wurde 1987 gegründet und hat das Ziel, verständliche Standards zum Austausch und zur Integration von elektronischen Gesundheitsinformationen bereitzustellen. Das Hauptaugenmerk der Organisation liegt dabei auf den beiden Standards HL7 v2 und v3. Während HL7 v2 ein rein ASCII-basierter Standard ist, nutzt v3 eine XML-basierte Struktur um Informationen zu übermitteln. HL7 v2 arbeitet mit sogenannten Segmenten um die Struktur der Nachricht aufzubauen, diese Segmente enthalten wiederum Felder, in denen Daten gespeichert sind ([HL7 2010b]). Der Standard definiert, dass jedes Segment einer Nachricht durch einen aus drei Buchstaben bestehenden Code identifizierbar sein muss, entsprechend dieses Codes gelten Vorgaben für die Daten der Felder des Segmentes. Abbildung 3 zeigt den Aufbau eines solchen Segmentes anhand eines Patient Information Segmentes, welches zur Übermittlung persönlicher Daten eines Patienten genutzt wird.

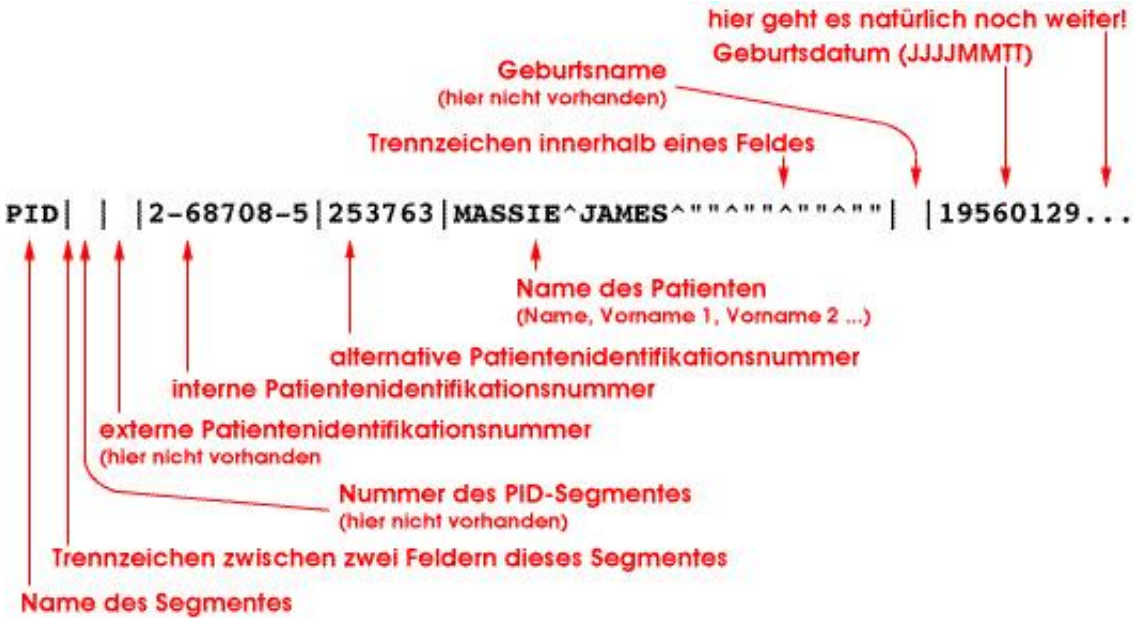

Abbildung 3: HL7 v2 PID Segment aus [HL7 2010b]

Durch die Verwendung von Segmenten und Feldern in einer flachen Datenstruktur beschreibt der Standard keine syntaktischen Regeln. Daher ist es alleine anhand der Daten

nicht möglich festzustellen, ob eine Nachricht korrekt konstruiert wurde. Dass HL7 v2 nicht gleichermassen Information sowohl über Inhalt als auch Struktur enthält, wurde als beschränkend empfunden. Die HL7 Organisation sah deshalb nur die Möglichkeit durch Entwicklung eines komplett neuen Standards Abhilfe zu schaffen, und v2 aufgrund von Kompatibilität und bereits großer Verbreitung seperat weiter zu unterstützen. In HL7 v3 wurde das Konzept der Datenmodellierung in den Standard eingebracht. XML wurde für die Struktur gewählt, welche nun über mehrere Ebenen an Modellierungsinformationen verfügt. Im Zuge der Entwicklung des neuen Standards wurde auch darauf geachtet, striktere Bedingungen an die Struktur der Nachricht zu stellen, um den Standard transparenter zu machen. Durch die Nutzung von XML wurde es jedoch zugleich einfacher, neue Erweiterungen einzuführen ([HL7 2007]).
Im Zuge der Entwicklung von HL7 v3 wurde auch das Reference Information Model entwickelt. RIM ist ein statisches Model, welches die Sicht auf Gesundheitsinformationen im Hinblick auf den HL7 Standard ermöglicht. Dieses Modell ist eine kritische Komponente im Entwicklungsprozess von HL7 v3. Aus diesem Modell werden alle Informationsmodelle und Strukturen als Teil des HL7 v3 Entwicklungsprozesses abgeleitet. Es enthält zu diesem Zweck unter anderem Zustands- und UseCase-Diagramme, Terminologien und Datenmodelle. HL7 fordert, dass alle Modelle, welche im Zuge von HL7 v3 entwickelt werden, auf das RIM zurückgeführt werden können müssen und dass die Rahmenbedingungen des RIM nicht verletzt werden. Das RIM eigenet sich daher zum Beispiel zur Erweiterung und Anpassung von HL7 v3 an lokale Gegebenheiten ([HL7 2006]).
HL7 v3 hat sich jedoch bisher nicht gegen v2 durchsetzen können. Dies liegt vor allem an der Durchdringung, die v2 bisher am Markt erreicht hat. Eine Umstellung auf v3 scheint für viele Nutzer nicht rentabel, da zum einen viele alte Systeme nicht mit v3 arbeiten und so neue Produkte gekauft werden müssten, zum anderen die Umstellung mit erheblichen Kosten und Ausfallzeiten verbunden wäre ([HL7 2007]). Neben dem RIM zur Modellierung wurde auch ein Standard zur elektronischen Speicherung von klinischen Dokumenten für HL7 v3 entwickelt ([HL7 2005]).

2.3.4 Health Level Seven (HL7) - Clinical Document Architecture (CDA)

Die Clinical Document Architecture (CDA) ist ein ANSI-zertifizierter Standard für klinische Dokumente und ist Teil von HL7 v3 ([HL7 2010a]). Version 1.0 wurde im November 2000 veröffentlicht, Version 2.0 mit der HL7 2005 Normative Edition. CDA spezifiziert die Syntax elektronischer klinischer Dokumente, es bietet darüber hinaus eine Grundstruktur, welche für die Spezifikation der Semantik von elektronischen, klinischen Dokumenten genutzt wird. Es ist dabei möglich, jedwede Form von klinischem Dokument abzubilden, beispielsweise Arztbriefe, OP- oder Laborberichte. CDA basiert dabei, so wie HL7 v3 auf XML. Es ist jedoch möglich, auch nicht aus XML bestehende Daten in CDA Dokumen-

ten in entsprechenden Elementen zu speichern. CDA verwendet, wie im vorherigen Kapitel erläutert, wie alle Teilkomponenten von HL7 v3 das RIM als Informationsquelle und benutzt entsprechende Datentypen. CDA beschränkt sich darauf Dokumente zu definieren. Es macht keine Aussagen über die Form der Speicherung der Dokumente oder deren Transport. Letzteres ist in HL7 spezifiziert. Ebenso werden keinerlei Aussagen über die Erzeugung oder Verwaltung der Dokumente gemacht. CDA ist also ein reiner Dokumentenstandard ([HL7 2005]).
Ein CDA Dokument besteht aus einem Header und einem Body. Im Header sind die Metadaten des Dokumentes gespeichert. Er besteht aus drei Teilen, den Header Attributes, den Header Participants und den Header Relationships.
Abbildung 4 zeigt das Beispiel eines CDA Dokumentes Headers, weitere Beispiele finden sich unter [HL7 2005].

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="CDA.xsl"?>
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/voc" xmlns:xsi=
        "http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd">
        <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>
        <templateId root="2.16.840.1.113883.3.27.1776"/>
        <id extension="c266" root="2.16.840.1.113883.19.4"/>
        <code code="11488-4" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC"
        displayName="Consultation note"/>
        <title>Good Health Clinic Consultation Note</title>
        <effectiveTime value="20000407"/>
        <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
        <languageCode code="en-US"/>
        <setId extension="BB35" root="2.16.840.1.113883.19.7"/>
        <versionNumber value="2"/>
        <component>
                <structuredBody/>
        </component>
</ClinicalDocument>
```

Abbildung 4: HL7 CDA Header

Die Header Attributes beschreiben die Datenfelder der ClinicalDocument Klasse ([HL7 2005] 4.2.1).

Header Attributes	
Komponente	Beschreibung
.id	Beinhaltet die eindeutige ID eines klinischen Dokumentes.
.code	Dieser Code spezifiziert den genauen Typ dieses Dokumentes, Werte hierfür liefert LOINC (siehe S,19).
.title	Repräsentiert den Titel des Dokumentes.
.effectiveTime	Zeitpunkt zu dem dieses Dokument erstellt wurde.
.ConfidentialityCode	Beinhaltet Informationen über Zugriffbeschränkungen, denen dieses Dokument unterliegt. Dieses Attribut kann drei Werte annehmen: N für Zugriff gemäß Good Healthcare Practice. Nur autorisierte, z.B. im Rahmen des Behandlungsvertrages, Personen dürfen auf dieses Dokument zugreifen. R für beschränkten Zugriff, zum Beispiel nur für Leistungserbringer, welche den Patienten aktuell behandeln. V für stark beschränkten Zugriff.
.languageCode	Sprache, in welcher das Dokument verfasst wurde.
.setId	ID, welche in allen Revisionen des Dokumentes vorhanden ist.
.versionNumber	Attribut für die fortlaufende Versionierung von neuen Dokumenten, welche dieses Dokument ersetzen.

Die Header Participants beschreiben die einzelnen mitwirkenden Personen, welche bei der Entstehung dieses Dokumentes eine Rolle spielen ([HL7 2005] 4.2.2).

Header Participants	
Komponente	Beschreibung
Authenticator	Repräsentiert eine beteiligte Person, welche die Richtigkeit des Dokumentes bezeugen, es aber aufgrund mangelender Privilegien nicht authentifizieren kann.
Author	Repräsentiert die Instanz, Mensch oder Maschine, welche das Dokument erstellt hat.
Custodian	Repräsentiert die Organisation, welche das Dokument verwaltet.

DataEnterer	Repräsentiert eine Person, welche an der Überführung einer diktierten Nachricht in Text beteiligt war, z.B. Sekretärin.
EncounterParticipant	Repräsentiert an dem Erstellungsgrund dieses Dokumentes beteiligte Personen.
Informant	Ein Informant ist eine Person, welche relevante Informationen bezüglich des Patienten zur Verfügung stellen kann.
InformationRecipient	Personen, die eine Kopie dieses Dokumentes erhalten sollten.
LegalAuthenticator	Person, welche das Dokument aus rechtlicher Sicht abgesegnet hat. (z.B. ein Assistenzarzt)
Participant	Personen, welche nicht in anderen Klassen genannt sind, jedoch in der Erstellung des Dokumentes involviert waren.
Performer	Personen, welche an den diesem Dokument zu Grunde liegenden Untersuchungen maßgeblich beteiligt waren.
RecordTarget	Repräsentiert die Patientenakte, zu der dieses Dokument gehört.
ResponsibleParty	Die Person, welche hauptsächlich rechtliche Verantwortung für den diesem Dokument zu grundeliegenden Erstellungsgrund trägt.
Participant Scenarios	Kann benutzt werden um Szenarien abzudecken, in denen mehrere hier aufgeführte Rollen von lediglich einer Person eingenommen werden.

Die Header Relationships enthalten Informationen zum Hauptdokument, zur Hauptuntersuchung, den Anordnungen und der zugeordneten Einwilligungserklärung ([HL7 2005] 4.2.3).

Header Relationships	
Komponente	Beschreibung
ParentDocument	Beschreibt das Dokument, auf dem die aktuelle Revision dieses Dokumentes aufbaut.
ServiceEvent	Dokumentiert die Hauptuntersuchung, kann dazu benutzt werden den Inhalt des ClinicalDocument.code weiter zu differenzieren.
Order	Repräsentiert die Anordnungen, die durch dieses Dokument ausgeführt werden.

Consent	Referenziert die Einwilligungserklärungen, die mit diesem Dokument assoziiert sind.
EncompassingEncounter	Angaben zum Kontext in dem die diesem Dokument zu Grunde liegenden Handlungen durchgeführt wurden.

Das Grundgerüst eines CDA Dokumentes ist in Abbildung 5 zu sehen. Dieses Beispiel beschränkt sich dabei auf wenige Strukturen und nicht alle vom Standard geforderten Komponenten sind vorhanden. CDA Dokumente sind grundsätzlich durch ein <ClinicalDocument> Element gekennzeichnet, welches den Header und den Body des Dokumentes enthält. Der Header ist dem <structuredBody> vorgestellt. In ihm werden die grundlegenden Information zur Natur und Identifikation des Dokumentes gespeichert. Zu diesen gehören beispielsweise der Patient und der Autor des Dokumentes. Der Body des Dokumentes enthält entweder in Markup strukturierte Informationen oder ist eine Ansammlung eines unstrukturierten Textes ([HL7 2005] 4.3.1). In Abbildung 5 ist der Body strukturiert und enthält eine beliebige Anzahl an <section> Elementen, in welchen <text> Elemente menschenlesbaren Text enthalten. <observation>, <substanceAdministration> und <supply> Elemente enthalten strukturierte Informationen für die weitere maschinelle Verarbeitung. Diese Elemente sind nur stellvertretend aufgeführt. Es sind noch weitere entry-level Elemente spezifiziert. Elemente diesen Typs enthalten typischerweise eine maschinenlesbare Präsentation des menschenlesbaren Textes und können in verschiedenen <section> Elementen beliebig oft auftreten ([HL7 2005] 4.3.6).

```
<ClinicalDocument>
        ... CDA Header ...
        <structuredBody>
                <section>
                        <text>...</text>
                        <observation>...</observation>
                        <substanceAdministration>
                                <supply>...</supply>
                        </substanceAdministration>
                        <observation>
                                <externalObservation>...
                                </externalObservation>
                        </observation>
                </section>
                <section>
                        <section>...</section>
                </section>
                ...
        </structuredBody>
</ClinicalDocument>
```

Abbildung 5: CDA Grundgerüst aus [HL7 2005]

Wie in Abbildung 5 ersichtlich, etabliert CDA eine Hierarchie aus mehreren Leveln. Diese Hierarchie formt eine Architektur. Die aktuelle Spezifikation besteht aus einem CDA XML Schema. Der Architekturaspekt wird durch die Möglichkeit, Dokumentenvorlagen zur Konstruktion der Dokumente zu verwenden, deutlich. Diese Vorlagen sollen die Freiheiten innerhalb von CDA begrenzen. Durch die Flexibilität von XML können diverse Vorlagen erstellt werden. Wichtig sind dabei besonders zwei Vorlagetypen. Vorlagen, welche das Dokument auf <section> Ebene beschränken und solche, welche auf entry-level innerhalb der <section> Elemente beschränken. Zusammenfassend gibt es drei Level in CDA 2.0 ([HL7 2005] 1.2.2):

◇ Level 1 ist die unbeschränkte Spezifikation. Text wird innerhalb von XML Elementen dargestellt und es gibt nur rudimentäre Möglichkeiten den Text zu formatieren. Dies ermöglicht begrenzte Interoperabilität, da Texte zwar repräsentierbar und lesbar, jedoch nicht maschinell auswertbar sind.

◇ Level 2 ist die Spezifikation mit Beschränkungen auf <section> Level. Es gibt Dokumentenvorlagen für bestimmte Sachverhalte, es ist möglich Code-Systeme, z.B. Logical Observation Identifiers Names and Codes[5] (LOINC), für die Beschreibung von Elementen heranzuziehen ([HL7 2005] 2.3). LOINC bietet allgemeine Codes und Namen um Laborwerte und andere klinische Observationen zu identifizieren. Durch die Dokumentenvorlagen sind Struktur und benötigte Informationen vorgegeben.

◇ Level 3 führt innerhalb der <section> Vorlagen weitere, maschinenlesbare, Elemente ein, in denen zum Beispiel Laborwerte repräsentiert werden können. Die entsprechenden Datentypen werden aus dem HL7 RIM entnommen und ermöglichen so Interoperabilität.

Dementsprechend ist es auch nur bedingt möglich CDA zu erweitern. Der Standard selbst lässt die Möglichkeit zu, sollte es für zu repräsentierende Informationen keine passende Repräsentation in CDA geben. Es muss jedoch weiterhin möglich sein, das Dokument ohne Kenntnis der neuen Schemata lesen und verarbeiten zu können. HL7 fördert das Einreichen eigener Ausarbeitungen für noch nicht erschlossene Themenbereiche, so dass diese in neueren Versionen allen Mitgliedern zugänglich gemacht werden können ([HL7 2005] 1.4).

[5] *http://loinc.org*

2.3.5 Organisation for the Advancement of Structured Information Standards (OASIS)

Die Organisation for the Advancement of Structured Information Standards (OASIS) ist ein gemeinnütziges Konsortium, das sich der Entwicklung und Adaption neuer offener Standards für die globale Informationsgemeinschaft verpflichtet hat. Das Konsortium stellt Standards für Sicherheit und e-Business zur Verfügung und betreibt Initiativen im öffentlichen Bereich sowie in anwendungsspezifischen Märkten. OASIS ist vorallem durch Tranparenz und flache Hierarchien gekennzeichnet. Neue Standards werden in einer offenen Abstimmung ratifiziert. Die Wahl der Board-Direktoren und des Technical Advisory Boards erfolgt alle zwei Jahre demokratisch und beruht auf den Leistungen der Individuen und nicht ihrer finanziellen Spenden. OASIS wurde 1993 unter dem Namen SGML Open als Konsortium von Anbietern und Nutzern gegründet, um Richtlinien für die Interoperabilität von Produkten zu entwickeln, welche die Standard Generalized Markup Language (SGML), einen Vorläufer der extensible Markup Language (XML), unterstützen. 1998 änderte OASIS seinen Namen um seinem erweiterten Betätigungsfeld Rechnung zu tragen, besonders im Hinblick auf die Entwicklungen im Bereich XML und anderer verwandter Standards. OASIS betreibt zum Zeitpunkt dieser Arbeit unter anderem zwei Webseiten für XML[6][7] und ist der Herausgeber der eXtensible Access Control Markup Language ([OASIS 2010]).

2.3.6 OASIS - eXtensible Access Control Markup Language (XACML)

Die eXtensible Access Control Markup Language (XACML), welche vom OASIS Konsortium entwickelt wird, ist ein auf XML basierender Standard zur Regelung von Zugriffsberechtigungen. Der Standard wurde im Hinblick auf die heterogene Landschaft der propiertären, sowie anwendungsspezifischen Standards für Zugriffsberechtigungen entwickelt ([OASIS 2010]). XACML versucht Interoperabilität zu ermöglichen. Der Standard beschreibt daher nicht nur die Syntax der Zugriffsberechtigungen sondern auch das Konzept zur Implementierung der Regelung des Zugriffes auf beliebige Ressourcen. Trotz der Vorgaben des Standards ist es möglich, eigene Anforderungen gezielt umzusetzen, da der Standard es zum Beispiel unter anderem ermöglicht, rollenbasierten oder dynamischen Zugriff zu implementieren. Grundgerüst hierfür sind die sogenannten, in XML forumulierten, Policies und das PolicySet, welche die benötigten Informationen für eine Regelung des Zugriffes auf eine Ressource enthalten ([XACML 2005] 2. - 2.8).

Von zentraler Bedeutung für die Regelung des Zugriffs durch einen Akteur auf eine Ressource ist das bereits im Standard definierte Konzept des Datenflusses, dargestellt in Abbildung 7. Für den Datenfluss ist dabei das Vorhandensein mehrerer Teilkomponenten entscheidend.

[6] *http://xml.coverpages.org/*
[7] *http://www.xml.org/*

Der Policy Administration Point (PAP) ermöglicht es, Policies oder PolicySets zu erzeugen. Diese werden im Policy Decision Point (PDP) evaluiert. Hierfür werden die Parameter der Anfrage von außen mit den Parametern der Policy verglichen. Sollten die Parameter übereinstimmen, so wird die Policy auf die Anfrage angewandt und das Ergebnis der Authorisierungsentscheidung an den Policy Enforcement Point (PEP) weitergegeben. Im PEP wird der Zugriff gemäß der Policies durchgesetzt. Dies geschieht durch Anfragen an die anderen bereits genannten Teilkomponenten und das Durchsetzen der Authorisierungsentscheidungen. Sollten weitergehende Informationen für eine Authorisierungsentscheidung benötigt werden, so werden diese über den Policy Information Point (PIP) abgefragt. Der Context Handler formuliert die eintreffenden Anfragen dabei in eine XACML konforme Form um. Ebenso werden ausgehende Nachrichten aus der XACML-Form in die Form der Ursprungsnachricht übersetzt ([XACML 2005] S,8 - S,9).

XACML wurde mit dem Ziel entwickelt, in diversen Anwendungsumgebungen eingesetzt werden zu können. Daher ist der eigentliche XACML Kern, in Abbildung 6 grau schattiert, von der Umgebung getrennt. Innerhalb des Kerns sind alle Ein- und Ausgaben der jeweiligen Komponenten vorgegeben. Daten, die von außerhalb des Kerns bezogen werden, müssen daher entsprechend in eine Repräsentation für XACML umgewandelt werden. Der Standard macht für diesen Vorgang allerdings keine Vorgaben ([XACML 2005] S,18).

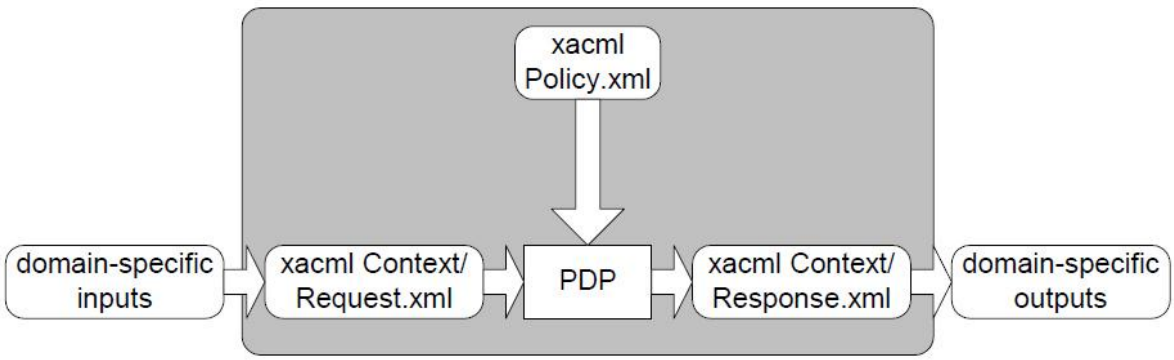

Abbildung 6: XACML Kontext aus [XACML 2005] S,18

Das Model (Abbildung 7) operiert dabei wie folgt:

1. Der PAP schreibt PolicySets, sowie Policies, und stellt sie für den PDP zur Verfügung. Diese Policies stellen die kompletten Regeln für den Zugriff auf eine Ressource zur Verfügung.

2. Eine Anfrage wird von einem System, welches Zugriff auf eine Ressource, beispielsweise eine Patientenakte, benötigt, an den PEP gesendet. Die Form der Anfrage ist dabei von XACML entkoppelt.

3. Der PEP sendet die Anfrage nach Zugriff an den Context Handler in seiner ursprünglichen Form, optional mit Attributen, welche für die Authorisierungsentscheidung benötigt werden.

4. Der Context Handler erzeugt eine, in XACML, formulierte Anfrage und leitet diese an den PDP weiter.

5. Der PDP fragt alle zusätzlichen benötigten Subject, Resource, Action und Environment Attribute beim Context Handler nach.

6. Der Context Handler fragt diese Attribute beim PIP nach.

7. Der PIP beschafft diese Attribute.

8. Der PIP gibt die Attribute an den Context Handler weiter.

9. Optional gibt der PIP die Resource an den Context Handler weiter.

10. Der Context Handler sendet die geforderten Attribute, und optional die Resource, an den PDP, welcher dann die Policy auswertet

11. Der PDP gibt den Antwort Context, zusammen mit der Authorisierungsentscheidung, an den Context Handler.

12. Der Context Handler formatiert den Antwort Context in das Format der Anfrage für den PEP um und gibt die Antwort dann an den PEP weiter.

13. Der PEP erfüllt die mit der Entscheidung einhergehenden Pflichten.

14. Wenn die Authorisierungsentscheidung positiv ausfällt, wird dem Anfragesteller durch den PEP Zugriff auf die Ressource gewährt, anderfalls wird der Zugriff verweigert.

Die bereits angesprochene Policy kann dabei Teil eines PolicySets sein, welches mehrere Policies enthält und dementsprechend komplexe Zugriffsberechtigungen enthalten kann. Ein PolicySet kann auch weitere PolicySets enthalten. Innerhalb einer Policy gibt es Rules, welche die eigentliche Entscheidung über den Zugriff enthalten. XACML definiert im sogenannten Policy Language Model (Abbildung 8) folgende Elemente ([XACML 2005] S,19ff):

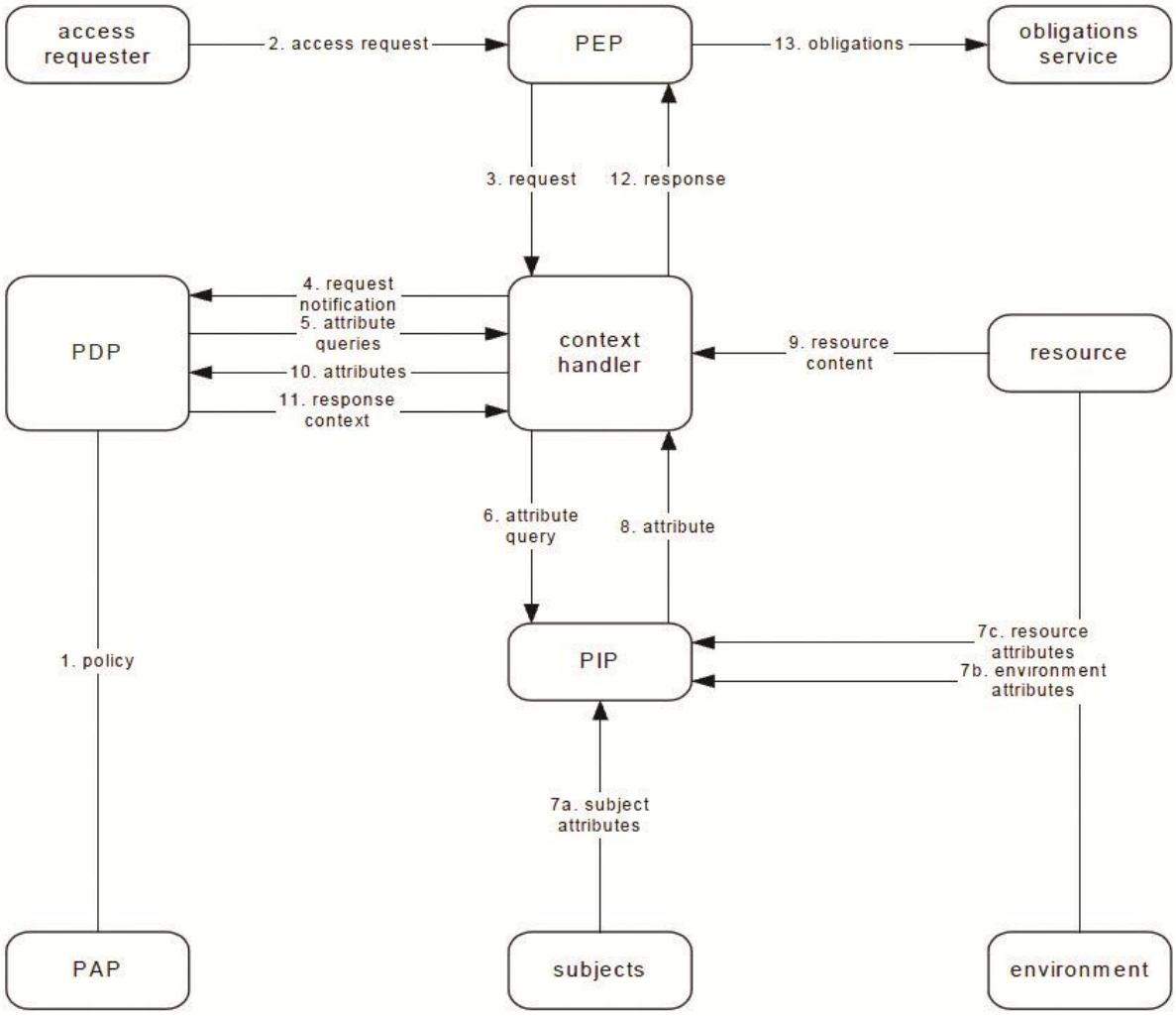

Abbildung 7: XACML Data-flow Model aus [XACML 2005] S,17

◇ **Target-Element** - Dieses Element beinhaltet Informationen über die Anwendungsfälle, auf die ein PolicySet, eine Policy oder eine Rule anwendbar sind. Alle drei Komponenten enthalten ein Element diesen Types. Das Target-Element besteht aus Subject-, Resource-, Action- und Environment-Elementen.

◇ **Subject-Element** - Dieses Element beinhaltet Informationen über die Personen, Personengruppen oder Organisationen, für die das Target-Element Gültigkeit besitzt.

◇ **Resource-Element** - Dieses Element beschreibt die Resource, für die der Zugriff beschränkt werden soll.

◇ **Action-Element** - Das Action-Element beschreibt für welche Aktionen, beispielsweise read und write, der Zugriff beschränkt wird.

◇ **Environment-Element** - Dieses Element kann zusätzliche Attribute, welche für die Entscheidungsfindung benötigt werden, enthalten.

◇ **Rule-Element** - Dieses Element beinhaltet maximal ein Condition-Element und genau ein Effect-Element.

◇ **Condition-Element** - Dieses Element ist eine boolsche Funktion welche Informationen aus dem Target-Element evaluiert.

◇ **Effect-Element** - Der Effekt, der von der Rule ausgeht. Kann die Werte permit oder deny annehmen.

Eine Policy greift nur, wenn die Informationen im vorliegenden Request und im Target Element übereinstimmen. Nicht präsente Elemente stehen für beliebige Werte. Dies ermöglicht es, den Zugriff auf eine Ressource so fein oder grob wie möglich festzulegen.
Innerhalb der Policy gibt es eine beliebige Anzahl an Rules, welche die eigentliche Entscheidung über den Zugriff beinhalten. Rules enthalten gleich der Policy ein Target-Element wodurch einzelne Zugriffsszenarien abgebildet werden können, die innerhalb der Policy auftreten können. Rules beinhalten optional ein Condition-Element, welches den Zugriff von bestimmten Vorfaktoren abhängig macht. Dies können zum Beispiel Uhrzeit oder Datum sein. Pflicht für jede Rule ist ein Effect-Element, welches für die Auswertung der Rule von Bedeutung ist. In diesem Element ist die Entscheidung über den Zugriff gespeichert ([XACML 2005] S,58).
Um eine Entscheidung bezüglich mehrerer Rules, innerhalb einer Policy, treffen zu können, gibt es in XACML sogenannte Rule-combining Algorithmen. Diese beschreiben, welches Verhalten beim Auftreten mehrerer Regeln abgebildet werden muss. Es gibt dabei drei Gruppen dieser Algorithmen. Zum einen Deny- und Permit-overrides, sortiert oder unsortiert. Dies sind Algorithmen, bei denen das Auftreten eines Denys oder eines Permits dazu führt, dass diese Entscheidung, unabhängig von Ergebnissen anderer Regeln, zu einer negativen oder positiven Entscheidung bezüglich des Zugriffs führt. Zum anderen First-applicable, hier ist das Ergebnis der ersten anwendbaren Regel das Ergebnis der Policy. Regeln, die danach noch anwendbar sein könnten, werden nicht weiter beachtet. Wie für Rules gibt es die selben combining Algorithmen auch für Policies, welche in einem PolicySet erforderlich sind. Zusätzlich gibt es für PolicySets allerdings noch den Algorithmus Only-one-applicable, alle Policies werden evaluiert und abschliessend betrachtet. Sollte nur eine anwendbare Policy gefunden worden sein, so wird ihr Ergebnis als Ergebnis der Policy zurückgegeben. Sollten jedoch mehrere Policies auf die Anfrage anwendbar sein, so wird als Ergebnis indeterminate zurückgegeben, bei keiner anwendbaren Regel not applicable. Beide Fälle erfordern eine gesonderte Betrachtung gemäß einer strikten oder laxen Zugriffspolitik ([XACML 2005] S,138).

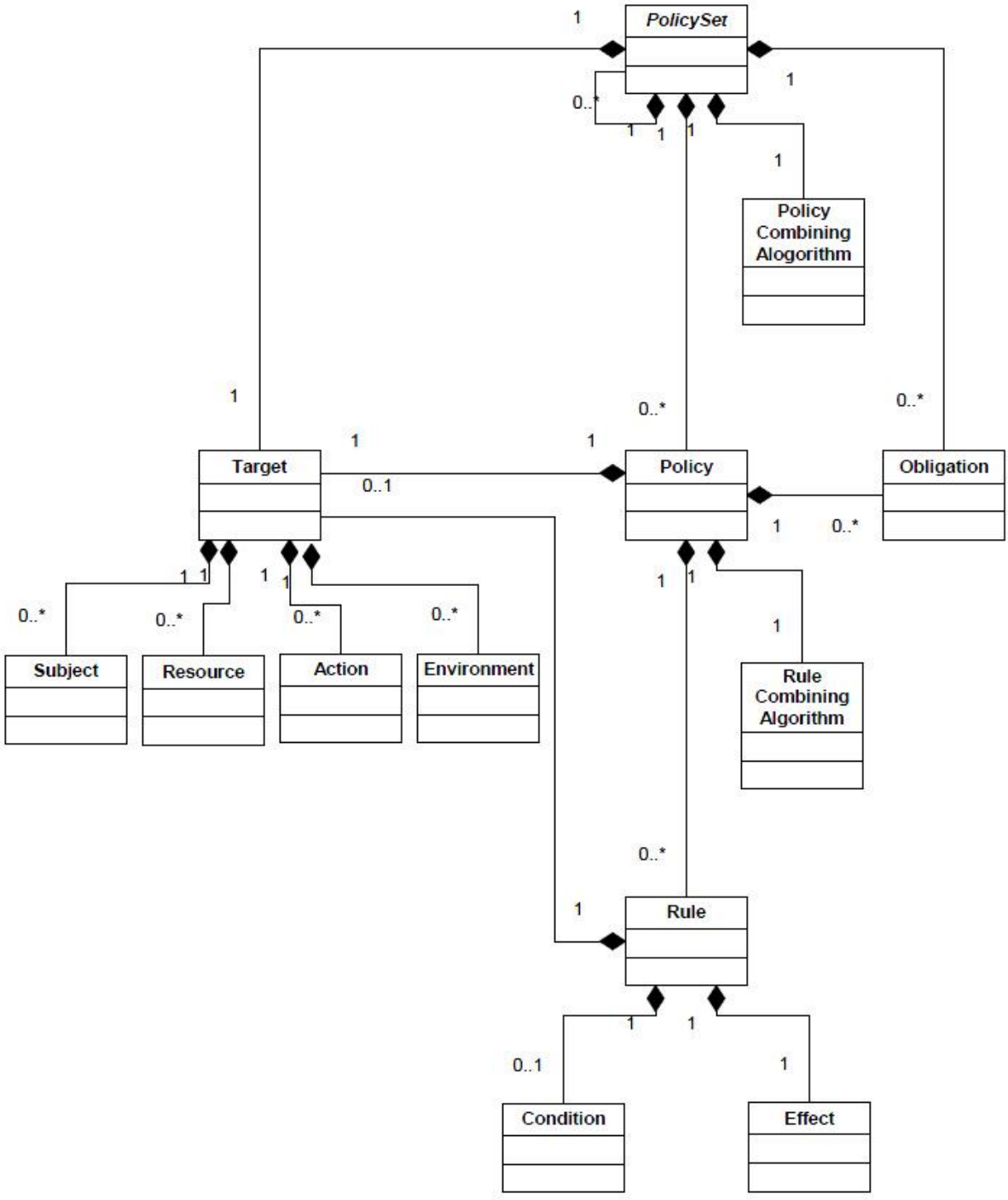

Abbildung 8: XACML Policy Language Model aus [XACML´2005] S, 19

2.3.7 Integrating The Healthcare Enterprise (IHE)

Integrating The Healthcare Enterprise (IHE) ist eine gemeinnützige Initiative, welche das Voranschreiten der Integration von Informationssystemen in medizinischen Organisationen zum Ziel hat. IHE operiert international und hat Suborganisationen in Europa, Nordamerika und Asien. IHE will es Nutzern und Entwicklern von Gesundheitstechnologien ermöglichen, Interoperabilität durch die präzise Definition von Aufgaben und die Spezifikation von Standard-basierter Kommunikation zu erreichen. Wichtigstes Ziel ist dabei, den medizinischen Entscheidungsträgern alle benötigten Informationen zur richtigen Zeit korrekt zur Verfügung zu stellen. IHE spezifiziert die Rahmenbedigungen für die Implementierung von etablierten Standards um klinische Ziele zu erreichen. Die Initiative ist dabei sowohl ein Prozess als auch ein Forum für Integrationsbemühungen. IHE Aktivitäten fallen daher in zwei Kategorien, zum einen „development activities“, Aktivitäten welche zur Formulierung der Implementierungsrichtlinien führen, zum anderen „deployment activities“, welche regionale oder nationale Demonstrationen der Ergebnisse des Entwicklungsprozesses sowie Tests der Implementierungen der Ergebnisse beinhalten ([IHE 2010a]). Zusätzlich organisiert IHE Ausstellungen und Workshops im Rahmen von Tagungen medizinischer Experten. Dies hat zum Ziel die Vorteile von IHE zu zeigen und die Teilnehmer zur Implementierung anzuregen ([IHE 2009a] S,7).
IHE beschränkt sich darauf bereits existierende Standards einzusetzen, beispielsweise HL7, OASIS und andere hinzuzufügen, wo dies nötig ist. Die eingesetzten Standards werden teilweise in ihren Konfigurationen zusätzlich beschränkt um Interoperabilität zwischen den verschiedenen beteiligten Akteuren zu gewährleisten. Sollte ein Standard nicht in der Lage sein die Anforderungen, welche ein IHE Profil an ihn stellt, zu erfüllen, so übermittelt IHE dem Herausgeber des Standards seine Empfehlungen diesbezüglich ([IHE 2009a] S,9).
Das Konzept von IHE basiert dabei auf Profilen, IHE Profile definieren standard-basierte Rahmenbedigungen für den Informationsaustausch zwischen den Beteiligten und deren Kommunikation über Netzwerke. Die Profile beinhalten Richtlinien für den Zugriff auf Informationen, klinische Prozesse, Sicherheit, Verwaltung und IT Infrastruktur. Jedes Profil definiert Akteure, Transaktionen und benötigte Informationen um den Standard zu finden, der mit diesem Anwendungsfall assoziiert wird. IHE Profile werden in sogenannten Technical Frameworks zusammengefasst. Sie dienen als technische Dokumentation für die Implementierung und sind frei erhältlich. Die Frameworks werden dabei von Kommitees innerhalb von Domänen entwickelt, eine Domäne umfasst dabei einen Teilbereich der Medizin und kann diverse Profile enthalten ([IHE 2010b]).
Zum Zeitpunkt dieser Arbeit wurden bereits folgende Domänen etabliert:

- ◇ Anatomic Pathology
- ◇ Cardiology

◇ Eye Care

◇ Laboratory

◇ Patient Care Coordination

◇ Patient Care Devices

◇ Radiation Oncology

◇ Radiology

◇ IT Infrastructure

Um zu überprüfen, ob IHE Profile der jeweiligen Domänen korrekt implementiert wurden, veranstaltet IHE den Connectathon ([IHE 2010c]). Auf dieser Tagung testen die Teilnehmer ihre Implementierung der IHE Profile gegeneinander und können so sicherstellen, dass ihre Implementierung korrekt ist und Interoperabilität gewährleistet. Ergebnisse des Connectathons sowie die Integration Statements, welche Aussagen über den Umfang der Implementierung der Profile in den Produkten machen, können auf der IHE Webseite[8] eingesehen werden. Auf der IHE Webseite können zudem die, für die Implementierung benötigten, Frameworks der spezifizierten Domänen heruntergeladen werden.

Das IHE IT Infrastructure Technical Framework (ITI TF) definiert Implementierungen für etablierte Standards um mit ihnen Integrationsziele zu erreichen, die das Übermitteln von Informationen zum Zweck der Patientenversorgung als Ziel haben. IHE ITI identifiziert Komponenten einer Gesundheitsorganisation, genannt IHE Akteure, und beschreibt deren Möglichkeiten zur Interaktion als ein Set von Transaktionen. Das IHE ITI fasst diese Transaktionen in Integrationsprofilen zusammen, in denen ihre Möglichkeiten Problemstellungen der IT zu lösen hervorgehoben werden.
In Version 6.0 der Frameworks werden neun Profile definiert:

◇ Patient Demographics Query (PDQ) - Ermöglicht es verteilten Anwendungen Patienteninformationen bei einem zentralen Server nachzufragen.

◇ Audit Trail and Node Authentication (ATNA) - Beschreibt die Charakteristika eines sicheren Netzwerkknotens.

◇ Personnel White Pages (PWP) - Ermöglicht den Zugriff auf Basisinformationen der Mitarbeiter.

[8] *www.ihe.net*

◇ Cross-Enterprise Document Sharing (XDS) - Ermöglicht es Mitgliedern einer XDS Affinity Domain (siehe Glossar - Anhang A) Dokumente eines Patienten miteinander auszutauschen.

◇ Cross-Enterprise User Assertion Profile (XUA) - Ermöglicht es Benutzer über Organisationsgrenzen hinaus zu authentifizieren.

◇ Patient Administration Management (PAM) - Stellt Transaktionen für Registrierung und Management von Patienten zur Verfügung, auch über Organisationsgrenzen hinaus.

◇ Cross-Enterprise Document Media Interchange (XDM) - Ermöglicht den Austausch von Dokumenten über mehrere, auch physische, Medien.

◇ Cross-Enterprise Sharing of Scanned Documents (XDS-SD) - Assoziiert strukturierte Gesundheitsmetadaten mit allgemeinen Dokumentenformaten um die Integrität, durch das Quellsystem verwaltet, der EPA zu gewährleisten.

◇ Basic Patient Privacy Consents (BPPC) - Ermöglicht es Einwilligungen des Patienten festzuschreiben, bietet Möglichkeiten Dokumente, welche in einer XDS Domäne publiziert wurden, mit der entsprechenden Einwilligung zu kennzeichnen und entsprechend den Zugriff zu beschränken.

2.3.8 IHE - Basic Patient Privacy Consent Module (BPPC)

Das Basic Patient Privacy Consent (BPPC) Profil zur Realisierung des Einwilligungsmanagements ist Teil der ITI Domäne. Bei seiner initialen Einführung war es ledliglich innerhalb der Patient Care Coordination (PCC) Domäne integriert. 2007 wurde es jedoch in die ITI Domäne überführt und seine endgültige Version 2008 vorgestellt ([IHE 2010b]).
Durch die XD* Profile wird der Austausch und die Nutzung der Dokumente eines Patienten möglich. Entsprechend ist es jedoch nötig den Zugriff zu beschränken. Das BPPC Profil stellt Möglichkeiten zur Verfügung, die Einwilligungen eines Patienten zu speichern ([IHE 2009a] S,132). Mittels dieser gespeicherten Einwilligungen ist es möglich, Dokumente, welche in einer XDS Domäne veröffentlich wurden und von einer Einwilligung betroffen sind, durch die Zuweisung einer OID (siehe Glossar - Anhang A) zu markieren und den Zugriff entsprechend der Einwilligung über das BPPC Profil zu beschränken. Dieses Profil komplettiert XDS dahingehend, dass es Funktionen bietet, durch die eine XDS Affinity Domain (AD) Einwilligungen entwickeln und implementieren kann. Zusätzlich beschreibt BPPC wie diese Funktionen mit den Zugriffsfunktionen der XDS Akteure integriert werden können.

Sollte das BPPC Profil nicht implementiert werden, so ist es nötig, dass der Administrator der XDS AD jeder Veröffentlichung und Nutzung eines Dokumentes explizit zustimmt und eine entsprechende Einwilligung erzeugt ([IHE 2009a] S,132). Eine solche Einwilligung wird durch die Zugriffsmechanismen der Teilkomponenten der XDS AD durchgesetzt.

BPPC orientiert sich an ISO 22600 - Privilege Management and Access Control (PMAC)[9], beschränkt sich aber nicht auf Systeme welche PMAC implementieren. Systeme, welche an XDS beteiligt sind, müssen ausreichende Zugriffskontrollen besitzen, um die Einwilligungen der XDS AD umsetzen zu können. ISO 22600 soll den Datenaustausch zwischen allen Beteiligten der Gesundheitsversorgung ermöglichen ([ISO 2010]). Hierfür definiert ISO 22600 Methoden, um den Zugriff auf Daten oder Funktionen zu verwalten. Konzeptionell basiert der Standard auf einem Modell, in dem lokale Authorisierungsserver und domänenübergreifende Daten- und Einwilligungsrepositories Softwarekomponenten dabei unterstützen ihren Zugriff zu regeln. Das Einwilligungsrepository stellt hierfür, basierend auf Rollen oder Attributen, Regeln für den Zugriff auf Daten oder Funktionen zur Verfügung, das Datenrepositroy stellt Informationen zur Identifikation von Benutzern bereit.

Die Grundidee hinter BPPC ist, dass es für Gesundheitsorganisationen oft nötig ist, Daten mehreren Interessengruppen teilweise auf unterschiedliche Art zu präsentieren. Beispielsweise verschiedene Sichten für Ärzte und Pflegepersonal, entsprechend der gegebenen datenschutzrechtlichen Bestimmungen. BPPC soll es ermöglichen, diese Daten in verschiedenen Dokumenten, welche mehreren Datenschutzregelungen unterliegen können, innerhalb einer XDS AD zu veröffentlichen. Hierfür stellt BPPC Funktionen zur Verfügung, mit denen es für eine XDS AD möglich wird, ein Basisvokabular zu erzeugen, mit dem Datenschutzregelungen im Hinblick auf Dokumentenaustausch identifiziert werden können. Inhalt der Datenschutzregelungen sind alle benötigten Informationen um den Zugriff zu regeln. Diese werden in einem rechtlich verbindlichen Text niedergeschrieben. In künftigen Versionen des Profils wird es vielleicht möglich sein, die Informationen des menschenlesbaren Textes in strukturierter Form abzulegen. BPPC benennt hierfür HL7 und OASIS als Ansatz, um noch dynamischer auf den Willen des Patienten eingehen zu können ([IHE 2009a] S,132). Wie in Kapitel 2.2 dargelegt, gibt es zwei Vorgehensweisen mit Einwilligungen, OPT-IN und OPT-OUT. BPPC unterstützt beide. Außerdem ist es möglich die gescannte Unterschrift des Patienten einzubinden ([IHE 2009a S,133]). Hierfür wird das XDS Scanned Document Content Profil genutzt. Abbildung 9 zeigt das Beispiel einer Einwilligungserklärung realisiert mittels CDA. Das BPPC Profil bietet einen Ansatz um Datenschutzregeln zu definieren, komplexe juristische oder organisatorische Anforderungen lassen sich aber möglicherweie nur schwer umsetzen. Vorgänge, bei denen ein Patient explizit dem Zugriff

[9] *http://www.iso.org/iso/catalogue_detail.htm?csnumber=36337*

zustimmen muss, oder zusätzliche Daten, über die der Datenschutzregel hinaus benötigt werden, stellen ein Problem dar. BPPC macht keine Aussagen, wie die zusätzlichen Informationen vorgehalten werden müssten, bietet in diesem Fall also eher eine Grundlage denn eine fertige Lösung ([IHE 2009a] S,135).

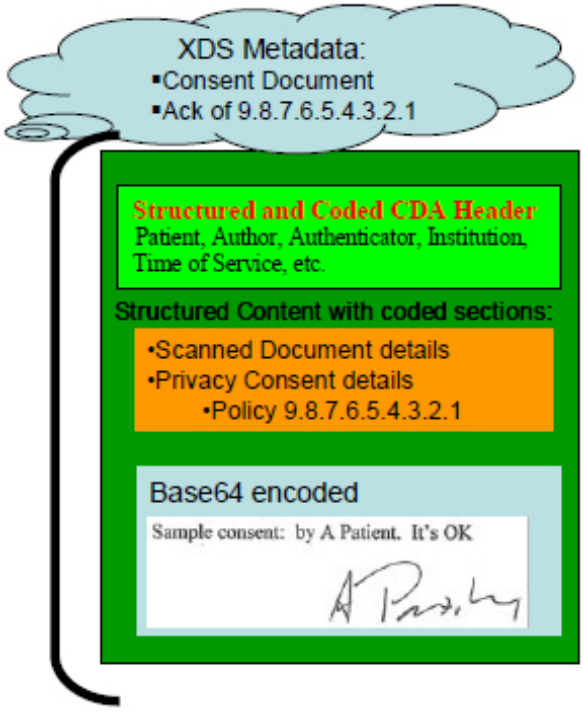

Abbildung 9: Konzept einer BPPC Einwilligung als HL7 CDA aus [IHE 2009a] S,135

Im Rahmen des Profils werden fünf Anwendungsfälle definiert. Die nachstehenden Beschreibungen sollen ihre Rolle innerhalb des Profils verdeutlichen:

Erzeugung von Datenschutzregelungen

Für den Betrieb einer XDS AD ist es dringend notwendig, eine Datenschutzregelung zu definieren und zu veröffentlichen, welche Aussagen über den allgemeinen, gültigen Gebrauch der XDS AD macht. Innerhalb dieser XDS AD Datenschutzregelung werden weitere Datenschutzregelungen definiert, denen der Patient zustimmen kann und die ihm eine Auswahl an Möglichkeiten bieten ([IHE 2009a] S,135). Über den Aufbau der Datenschutzregelungen oder deren Entwicklung macht das Profil keine Angaben, ebenso über den Mechanismus der Veröffentlichung dieser Dokumente. Allgemein fordert BPPC, dass die Datenschutzregelungen innerhalb der XDS AD als Set zusammengestellt werden können müssen. Durch

dieses Set soll es möglich sein, den Zugriff auf Dokumente oder deren Veröffentlichung, zu regeln, indem man die einzelnen Datenschutzregeln einzeln oder in Kombination betrachtet ([IHE 2009a] S,135). Eine einzelne Datenschutzregelung enthält Informationen bezüglich des durch die Datenschutzregelung betroffenen Personenkreises, sowie Informationen über die Daten, welche von ihr geschützt werden. Das Set der Datenschutzregelungen muss von allen Teilsystemen der XDS AD verarbeitet werden können. Es muss dementsprechend sorgsam entwickelt werden und auf Technologien der Systeme basieren ([IHE 2009a] S,136).
Jede Datenschutzregelung erhält einen Object Identifier (OID), über den in der XDS AD veröffentlichte Dokumente identifiziert werden. Durch diese Identifikation ist es möglich die zugeordnete Datenschutzregelung ausfindig zu machen. Zusätzlich wird der Identifier genutzt, um die Zustimmung eines Patienten zu einer Datenschutzregelung zu erfassen. Altdokumente enthalten möglicherweise keinen confidentialityCode (siehe Glossar - Anhang A), in dem die OIDs der Dokumente gespeichert werden. Entsprechend müssen Lösungen gefunden werden um diese Dokumente mit Zugriffsbeschränkungen zu versehen ([IHE 2009a] S,136). BPPC macht hierzu allerdings keine konkreten Vorgaben sondern stellt nur in Aussicht, dass es bei der Implementierung von BPPC an dieser Stelle zu Problemen kommen kann, die eigene Lösungen erfordern. Ebenso wird angemerkt dass es nötig sei Strategien für die sich ändernden Anforderungen an die Datenschutzregelungen zu entwickeln ([IHE 2009a] S,136).
BPPC stellt zusätzlich die Anforderung, die Zugriffskontrolle auf Seiten des Document Consumers zu implementieren. Diese Rolle fordert Dokumente aus der XDS AD an. Die Zugriffsbeschränkungen der XDS AD sind hierfür die Grundlage. BPPC begründet die Implemtierung der Zugriffskontrolle auf Seiten der Consumer damit, dass der Consumer am ehesten im Bilde darüber sei, in welcher Position er ist, wie die geplante Nutzung der Daten aussieht, das Verhältnis zwischen Gesundheitsdienstleister und Patient, die Rolle des Anwenders und dergleichen ([IHE 2009a] S,135).

Erzeugung einer Einwilligungserklärung

Sollte ein Patient einer im vorherigen Abschnitt beschriebenen Datenschutzregelung zustimmen, so wird diese als HL7 CDA Dokument vom sogenannten Content Consumer erzeugt. In diesem Dokument stimmt der Patient einer bestimmten Datenschutzregelung zu, zusätzlich kann das Dokument noch mit einer Signatur des Patienten versehen werden ([IHE 2009a] S,141).

Prüfung auf Vorliegen einer Einwilligungserklärung

Mittels BPPC kann ein Document Consumer durch Implementierung des optionalen Basic Patient Privacy Consent Proof innerhalb einer XDS AD nach Einwilligungserklärungen ei-

nes Patienten suchen. Durch die XDS Metadaten ist es dem Document Consumer möglich, einzusehen, welchen Datenschutzregelungen der Patient zugestimmt hat. Entsprechend ist es dem Document Consumer auch möglich, Informationen aus dem CDA Dokument, welches im Document Registry indiziert und im Document Repository gespeichert ist, auszulesen, zum Beispiel die gescannte Unterschrift oder die Details der Einwilligungserklärung ([IHE 2009a] S,141).

Veröffentlichung von Dokumenten gemäß einer Einwilligungserklärung

Wie bereits beschrieben, werden alle Dokumente der XDS AD mit einem confidentialtyCode versehen. Um Dokumente im Document Repository zu vermerken, ist ein confidentialityCode aus dem Vokabular der XDS AD zwingend notwendig. Das BPPC Profil ermöglicht es dem Administrator einer XDS AD, ein Vokabular zu schreiben und diesem Vokabular Bedeutung zu geben. Bei einer angestrebten Veröffentlichung eines Dokumentes prüft der Document Source Akteur unter welchen Datenschutzregelungen der XDS AD er ein Dokument veröffentlichen kann. Hierfür kann es notwendig sein zu prüfen, ob ein Patient einer Datenschutzregelung explizit zugestimmt hat. Im Falle einer Veröffentlichung werden die OIDs der Datenschutzregelungen, von denen das Dokument betroffen ist, im confidentialityCode der XDS Metadaten durch den Document Source Akteur vermerkt. Das XDS Repository stellt sicher, dass alle confidentialityCodes aus dem Vokabular der XDS AD stammen. Sollten bei einer angestrebten Veröffentlichung keine Einwilligungen gefunden werden so wird die Veröffentlichung durch den Document Source Akteur abgebrochen ([IHE 2009a] S,141).

Nutzung veröffentlichter Dokumente

Sollte ein Document Consumer einer XDS AD Dokumente bei ihr nachfragen, ist es möglich, die Menge der Dokumente durch Nutzung des confidentialityCode Filters zu reduzieren und auf jene zu beschränken, welche der Document Consumer nutzen kann. Nur diese werden dann an den Document Consumer zurückgegeben. Für eine solche Anfrage an die XDS AD wird das sogenannte Registry Stored Query genutzt. Zusätzlich zu diesem Ansatz gibt es noch die Möglichkeit, den confidentitalityCode direkt in der Registry Stored Query Transaction zu setzen. Der confidentialityCode wird auf die OIDs der Dokumente, welche es dem Document Consumer erlauben würden, das Dokument zu nutzen, gesetzt. Dadurch erhält der Document Consumer nur Informationen über Dokumente mit der angegebenen OID. Der Document Consumer beschränkt den Zugriff, basierend auf dem zurückgegebenen confidentialityCode der XDS Metadaten, des Benutzers, Kontext und jedwede andere Parameter, die es dem System ermöglichen eine Entscheidung zu treffen. Schlussendlich kann der Document Consumer auch alle bereits veröffentlichten Einwilligungserklärungen

eines Patienten anfragen und aus dieser Liste eine Liste der XDS Metadaten mit den Dokumenten erstellen, auf die er Zugriff hat. Anschließend kann er diese Dokumente bei der XDS AD nachfragen ([IHE 2009a] S,141).

Eingesetzte Akteure

Zusätzlich zu den Anwendungsfällen werden im BPPC Profil auch die Akteure für die Interaktion definiert, welche unter anderem in den Anwendungsfällen eine Rolle spielen ([IHE 2009a] S,138 Tabelle 19.3-1):

◇ **Document Source** - Erzeugt und veröffentlicht Dokumente, ist zudem verantwortlich für die Übermittelung von Dokumenten an das Document Repository. Zu diesem Zweck übermittelt die Document Source Metadaten, um es dem Document Repository möglich zu machen, das Dokument in der Document Registry zu registrieren ([IHE 2009a] S,71).
Zugeordnete Transaktionen: Provide and Register Document Set, Provide and Register Document Set-b
Zugeordnete Profiloptionen: Basic Patient Privacy Enforcement

◇ **Document Consumer** - Fragt beim Document Registry mittels des Registry Stored Query Dokumente nach, die bestimmte Kriterien erfüllen, und erhält diese von einem oder mehreren Document Repositories ([IHE 2009a] S,71).
Zugeordnete Transaktionen: Retrive Document, Retrieve Document Set, Registry Stored Query
Zugeordnete Profiloptionen: Basic Patient Privacy Proof

◇ **Document Recipient** - Der Document Recipient ist der Empfänger von Dokumenten im Rahmen einer XDR Transaktion. ([IHE 2009a] S,137).
Zugeordnete Transaktionen: Provide and Register Document Set-b
Zugeordnete Profiloptionen: Basic Patient Privacy Enforcement

◇ **Portable Media Creator** - Der Portable Media Creator fasst den Inhalt eines Datenträgers zusammen und schreibt diesen auf einen physischen Datenträger. Diesem Schritt geht die Extraktion der Dokumente aus dem EPA System vorraus ([IHE 2009a] S,149).
Zugeordnete Transaktionen: Distribute Document Set on Media
Zugeordnete Profiloptionen: Basic Patient Privacy Enforcement

◇ **Portable Media Importer** - Der Portable Media Importer liest die Daten aus einem Medium aus und stellt diese anschließend dar. Der Benutzer kann nun auswählen alle oder nur bestimmte Daten zu speichern. Allgemein werden solche Dokumente in ein EPA System integriert ([IHE 2009a] S,149).
Zugeordnete Transaktionen: Distribute Document Set on Media
Zugeordnete Profiloptionen: Basic Patient Privacy Enforcement

◇ **Content Creator** - Der Content Creator erzeugt Inhalte, die von einem Content Consumer verarbeitet werden können. Content Creator können zum Beispiel durch Document Source oder Portable Media Creator Akteure verkörpert werden. ([IHE 2009b] S,23).
Zugeordnete Transaktionen: Share Content
Zugeordnete Profiloptionen: Basic Patient Privacy Acknowledgement, Basic Patient Privacy Acknowledgement with Scanned Document

◇ **Content Consumer** - Der Content Consumer greift auf Dokumente innerhalb der XDS AD zu. Document Consumer, Document Recipient oder Portable Media Importer Akteure können einen Content Consumer verkörpern. ([IHE 2009b] S,23).
Zugeordnete Transaktionen: Share Content
Zugeordnete Profiloptionen: Basic Patient Privacy Acknowledgement View

Wie aus der Erklärung der BPPC Akteure ersichtlich ist, kommunizieren diese mit zwei Akteuren des XDS Profils, dem Document Repository und dem Document Registry (Abbildung 10).

◇ **Document Repository** - Das Document Repository ist für die transparente, sichere, zuverlässige und persistente Speicherung der Dokumente innerhalb der XDS AD verantwortlich. Des eiteren ist es seine Aufgabe auf Anfragen nach Dokumenten zu reagieren und diese an den Anfragesteller zurückzugeben ([IHE 2009a] S,68). Zu den Aufgaben des Document Repositorys gehört es auch, die Dokumente in der Document Registry zu registrieren. Zu diesem Zweck weist das Repository jedem Dokument einen Uniform Resource Identifier (URI) zu, durch diesen wird ein Dokument eindeutig identifizierbar und kann so durch Document Consumer angefragt werden ([IHE 2009a] S,72).

◇ **Document Registry** - Das Document Registry ist für die Speicherung der Informationen über die im Dokument Repository vorgehaltenen Dokumente verantwortlich ([IHE 2009a] S,68). Dies ermöglicht die vom Repository unabhängige Suche

nach Dokumenten. In der Registry werden die Metadaten der Dokumente vorgehalten, zu diesen Daten gehört unter anderem ein Link zu dem Repository, in dem sich das Dokument befindet [IHE 2009a] S,71). Die Registry antwortet auf Anfragen von Document Consumern.

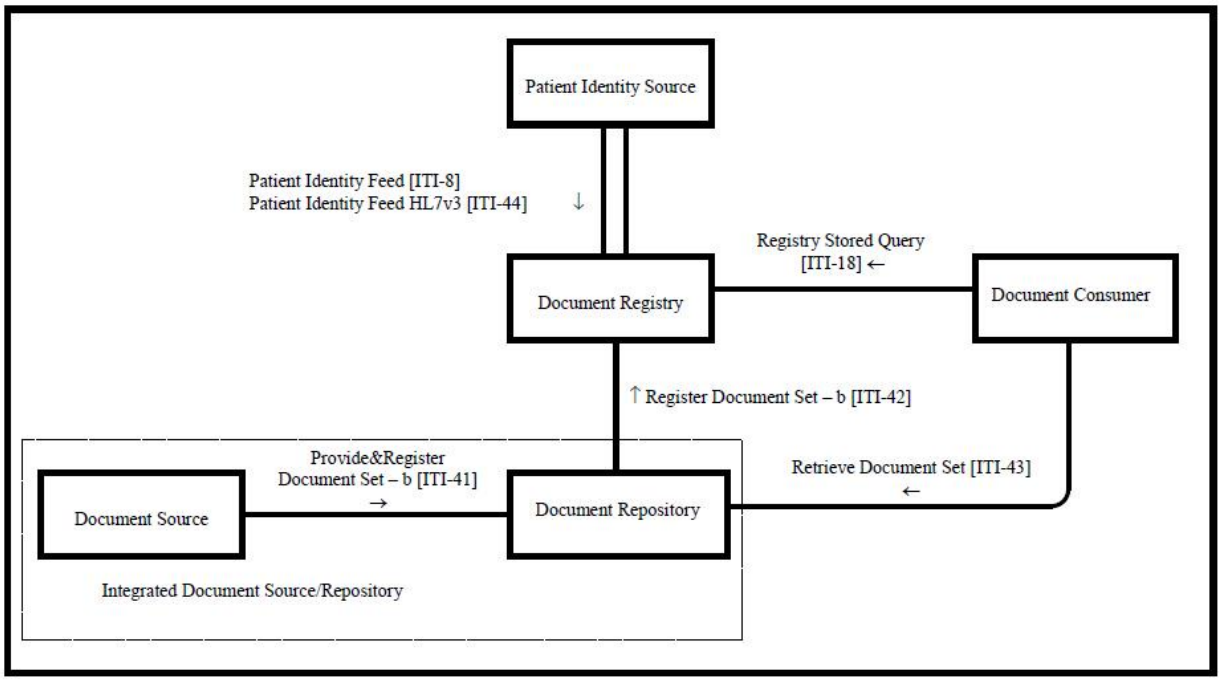

Abbildung 10: Cross-Enterprise Document Sharing (XDS.b) aus [IHE 2009a] S,70

Zwischen den Akteuren den BPPC-Profils laufen nur standardisierte Transaktionen ab. Möglich sind die folgenden Transaktionen ([IHE 2009a] S,72):

Eingesetzte Transaktionen

◇ **Provide and Register Document Set** - Diese Transaktion wird von einem Document Source Akteur initiiert. Für jedes Dokument, das Teil des Dokumentensets ist, stellt der Document Source Akteur sowohl einen Datenstrom als auch die Metadaten des Dokumentes dem Document Repository zur Verfügung. Das Repository ist für die Speicherung und die Registrierung der Dokumente in der Document Registry durch die Register Documents Transaktion verantwortlich. Letzteres geschieht durch die Weitergabe der Metadaten, die vom Document Source Akteur erhalten wurden, an die Document Registry ([IHE 2009a] S,72).
Aufrufende Akteure: Document Source, Document Recipient

◇ **Retrieve Document** - Diese Transaktion wird durch einen Document Consumer initiiert. Das Document Repository gibt das in der Anfrage spezifizierte Dokument zurück. Es ist möglich, dass ein XDS Dokument aus mehreren einzelnen Dokumenten aufgebaut ist. Der Empfänger muss einen solchen Fall entsprechend berücksichtigen ([IHE 2009a] S,73).
Aufrufender Akteur: Document Consumer

◇ **Retrieve Document Set** - Das durch einen Document Consumer angeforderte Dokumentenset wird durch das Document Repository an ihn zurückgegeben ([IHE 2009a] S,74).
Ausführende Akteure: Document Consumer

◇ **Registry Stored Query** - Die Registry Stored Query Transaktion wird durch einen Document Consumer im Auftrag eines Leistungserbringers initiiert und ist an die Document Registry adressiert. Die Document Registry durchsucht die Registry nach Dokumenten, die den in der Anfrage enthaltenen Spezifikationen entsprechen. Als Antwort erhält der Document Consumer eine Liste der Metadaten der Dokumente, welche die Spezifikation erfüllen. Zusätzlich enthält die Liste Informationen über die Repositories, in denen sich die entsprechenden Dokumente befinden sowie ihre Identifier ([IHE 2009a] S,73).
Aufrufender Akteur: Document Consumer

◇ **Distribute Document Set on Media** - Ein Quellakteur (Portable Media Creator) schreibt ein Dokumentenset auf einen austauschbaren Datenträger. Der Datenträger wird physisch zu einem anderen Akteur (Portable Media Importer) gebracht, welcher anschließend die Dokumente importiert oder als Anhang einer Email weitersendet. Das Medium kann auch an einen Patienten oder behandelnden Arzt weitergegeben werden um die Dokumente webbasiert zu betrachten ([IHE 2009a] S,153).
Aufrufende Akteure: Portable Media Creator, Portable Media Importer

◇ **Share Content** - Diese Transaktion dient dem Austausch von Daten zwischen einem Content Creator und einem Content Consumer ([IHE 2009a] S,137).
Aufrufende Akteure: Content Creator, Content Consumer

Zusätzlich zu diesen Transaktionen nutzt das BPPC Profil eine weitere essentielle Transaktion um den Ablauf der Anwendungsfälle möglich zu machen:

◇ **Register Document Set** - Diese Transaktion macht es dem Document Repository möglich, ein oder mehrere Dokumente in der Document Registry zu registrieren. Die übermittelten Metadaten werden genutzt um in der Regsitry einen XDS Document Entry zu erstellen. Die Document Registry stellt sicher, dass die übermittelten Metdaten valide sind, bevor das Dokument in die Registry eingebracht wird. Sollten ein oder mehrere Dokumente der Überprüfung nicht standhalten, so wird die gesamte Transaktion abgebrochen und kein Dokument des Sets eingebracht ([IHE 2009a] S,72).
Aufrufender Akteur: Document Repository

Neben den Pflichtbausteinen des Profils gibt es noch optionale Funktionsbausteine, die zusätzliche Funktionalität bieten, allerdings nicht zwingend implementiert werden müssen:

◇ **Basic Patient Privacy Enforcement** - Alle in einer XDS AD enthaltenen oder mittels XDM/XDR transferierten Dokumente enthalten einen confidentialityCode. Das BPPC Profil stellt eine Möglichkeit für den Administrator einer XDS AD dar, ein Vokabular für den confidentialityCode zu definieren und diesem Bedeutung zu geben. Akteure, welche diese Option in XDS, XDM oder XDR unterstützen, müssen bestimmte in diesen Profilen vermerkte Anforderungen erfüllen ([IHE 2009a] S,139).
Aufrufende Akteure: Document Source, Document Consumer, Document Recipient, Portable Media Creator, Portable Media Importer

◇ **Basic Patient Privacy Proof** - Um festzustellen, ob ein bestimmter Patient einer Datenschutzregelung zugestimmt hat, ist es einem Document Consumer möglich mittels der Registry Stored Query Transaktion nach Einwilligungserklärungen des Patienten zu suchen. Suchkriterium dieser Anfrage sollte die entsprechende Dokumentenklasse sein; consent. Durch die XDS Metadaten der Antwort ist es möglich, mittels der EventCodeList festzustellen, welchen Datenschutzregelungen zugestimmt wurde und über welchen Zeitraum diese Gültigkeit besitzen ([IHE 2009a] S,139).
Aufrufender Akteur: Document Consumer

◇ **Basic Patient Privacy Acknowledgement** - Jeder Content Creator, der die Basic Patient Privacy Acknowledgement Option unterstützt, muss in der Lage sein,

Einwilligungserklärungen erzeugen zu können. Eine Einwilligungserklärung stellt ein medizinisches Dokument dar, welches den Zeitraum der Erklärung des Einverständnisses sowie die OID der Datenschutzregelungen der XDS AD enthält, welchen mit diesem Dokument zugestimmt wurden. Die Einwilligung kann einen menschenlesbaren Text enthalten, der beschreibt, zu welchem Sachverhalt der Patient seine Zustimmung gegeben hat. Ebenso ist es möglich das Dokument zu signieren ([IHE 2009a] S,139).
Aufrufende Akteure: Content Creator

◇ **Basic Patient Privacy Consent Acknowledgement with Scanned Document** - Diese Option ermöglicht es ein gescanntes Dokument zur Einwilligungserklärung der vorherigen Option hinzuzufügen. Dementsprechend ist die vorherige Option zwingend für eine Implementierung dieser Option notwendig ([IHE 2009a] S,140).
Aufrufender Akteur: Content Creator

◇ **Patient Privacy Consent Acknowledgement View** - Jeder Content Consumer, der angibt diese Option zu unterstützen, muss in der Lage sein, Einwilligungserklärungen anzuzeigen ([IHE 2009a] S,140).
Aufrufender Akteur: Content Consumer

2.4 Elektronische Signatur

Die handschriftliche Unterschrift eines Menschen ist ein zentraler Teil der Bestätigung der Authentizität eines Dokumentes. Durch die Popularität des Internets werden immer mehr Vorgänge elektronisch abgewickelt, sei es im Bereich des E-Business oder E-Government ([BSI 2010]). Diese Vorgänge müssen ebenso dokumentiert werden wie ein handschriftlicher Vertragsschluss um rechtliche Gültigkeit zu besitzen. Der Gesetzgeber fordert in §67 Sozialgesetzbuch V *„papiergebundene Kommunikation unter den Leistungserbringern sobald und so umfassend wie möglich durch die elektronische und maschinell verwertbare Übermittlung von Befunden, Diagnosen, Therapieempfehlungen und Behandlungsberichten, die sich auch für eine einrichtungsübergreifende fallbezogene Zusammenarbeit eignet“* zu ersetzen. Es gelten dabei grundlegende Anforderungen an die übertragenen Informationen. Zum einen muss der Absender eindeutig identifizierbar sein. Dies wird ermöglicht durch Authentizität, die Echtheit des Dokumentes und Nichtabstreitbarkeit. Außerdem muss die Integrität der Daten gewährleistet sein, eine Manipulation durch Dritte muss ausgeschlossen werden können. An das elektronische Dokument werden zudem die Anforderungen

der Lesbarkeit, Vollständigkeit, Verkehrsfähigkeit und Verfügbarkeit gestellt ([DIG 2008]). Dies bedeutet, dass Dokumente jederzeit wieder lesbar gemacht werden können müssen. Das Dokument muss dabei vollständig sein und sein Beweiswert darf durch die Entnahme aus dem aufbewahrenden System nicht gemindert werden. Zudem muss die Entnahme zeitnah erfolgen können. Im Zuge der Entwicklung zu automatisch ablaufenden Vorgängen und zunehmender Digitalisierung von Dokumenten ist es durch die gesetzlichen Rahmenbedingungen, Dokumente handschriftlich zu unterschreiben, nötig, auch digitale Dokumente zu signieren ([BSI 2006] S,1). Die elektronische Signatur kann die genannten Anforderungen erfüllen, durch kryptografische Verfahren wird für den Empfänger ersichtlich, ob die Daten manipuliert wurden. Der Autor der Nachricht kann durch die Zuordnung der Signaturschlüssel zum Absender eindeutig identifiziert werden. Zusätzlich zu diesen Funktionen kann eine elektronische Signatur durch Zeitstempel den Zustand eines Dokumentes zu einem bestimmten Zeitpunkt festhalten. Um rechtlich verbindlich und damit beweisbar zu sein, sind diese Funktionen der elektronischen Signatur zwingend notwendig ([BSI 2010]). Der Gesetzgeber hat für Nutzung der elektronischen Signatur bereits Rahmenbedingungen definiert.

2.4.1 Rechtsgrundlagen

Das Signaturgesetz (SigG, [Bund 2009b]) und die ergänzende Signaturverordnung (SigV, [Bund 2001]) bilden die rechtliche Grundlage für elektronische Signaturen. Das SigG und die SigV definieren die Anforderungen an Zertifizierungsdienstanbieter, Produkte für elektronische Signaturen und die Prüfstellen, welche die Einhaltung der Gesetze durch die vorher Genannten überprüfen ([DIG 2010]). Das SigG definiert dabei verschiedene Typen (Abbildung 11) der elektronischen Signatur:
Nach §2 SigG sind:

> *1. "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,*
>
> *2. "fortgeschrittene elektronische Signaturen" elektronische Signaturen nach Nummer 1, die*
>
> > *a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,*
> >
> > *b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,*
> >
> > *c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und*
> >
> > *d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,*

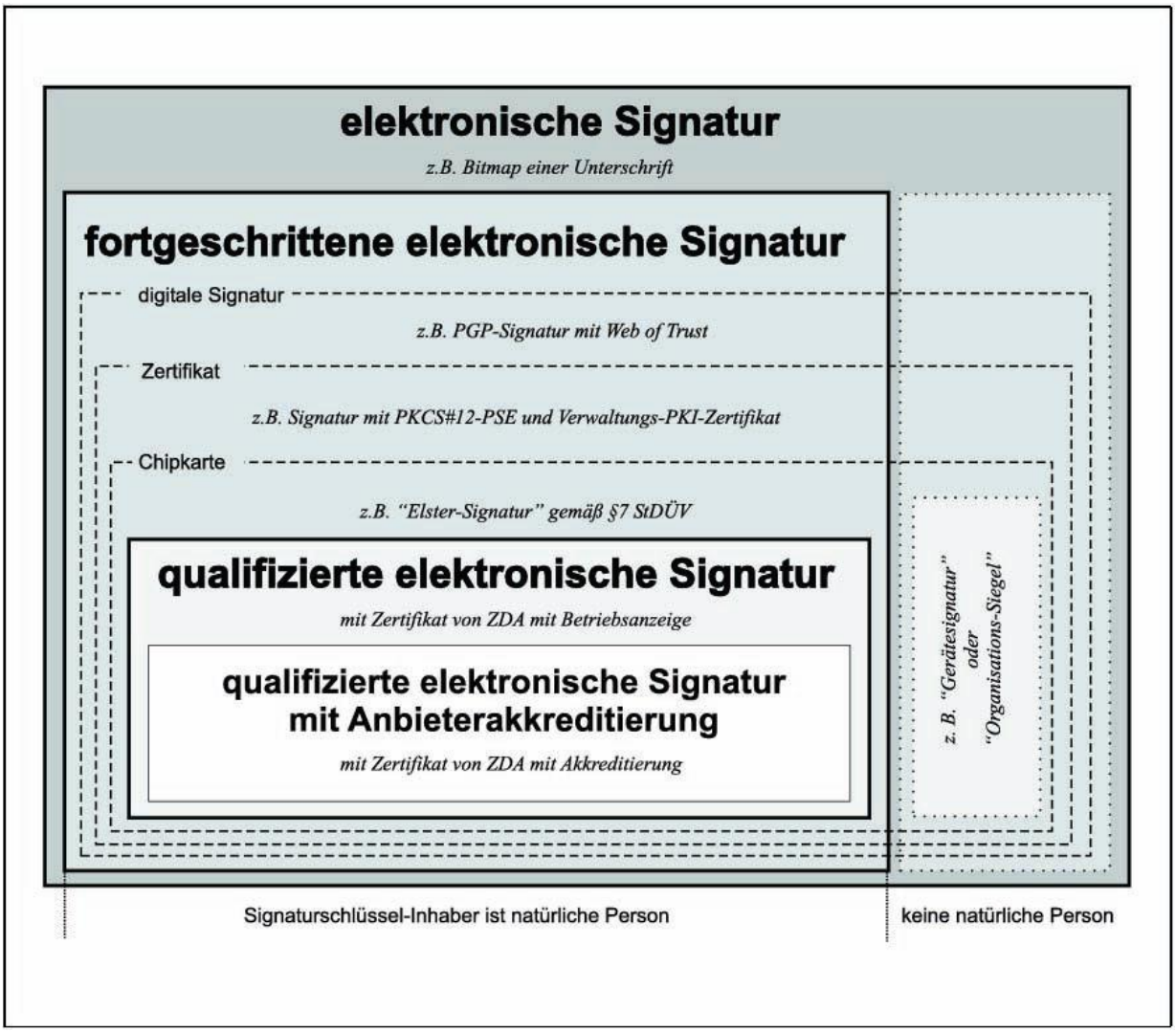

Abbildung 11: Arten der elektronischen Signatur aus [BSI 2006] S,8

3. "qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die

a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und

b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Die einfache elektronische Signatur soll es ermöglichen, den Absender einer Nachricht zu identifizieren. Dies kann beispielsweise durch das Einfügen einer gescannten Unterschrift geschehen. Für diese Art der Signatur sind keine Bedingungen an Sicherheit oder Fälschungssicherheit festgehalten. Dementsprechend bietet sie nur wenig Beweiskraft und Rechtssi-

cherheit. Der einzige Vorteil ergibt sich in der Erkennbarkeit des möglichen Absenders. Allgemeiner lässt sich eine einfache elektronische Signatur als elektronische Signatur definieren, welche nicht alle Anforderungen an eine fortgeschrittene elektronische Signatur erfüllt ([BSI 2006] S,119).
Eine fortgeschrittene elektronische Signatur ermöglicht es, nach §2 SigG, den Absender einer Nachricht eindeutig zu identifizieren, Authentizität und die Integrität der empfangenen Daten festzustellen. Dafür muss der Signaturschlüssel-Inhaber jedoch sicherstellen, dass sich sein Schlüssel unter seiner alleinigen Kontrolle befindet. Die fortgeschrittene elektronische Signatur besitzt daher der einfachen elektronischen Signatur gegenüber etwas mehr Beweiswert ([BSI 2010]). Die Erstellung einer fortgeschrittenen elektronischen Signatur erfolgt meist unter Verwendung von digitalen Signaturen und Zertifikaten, sie kann die Schriftform dennoch nicht ersetzen ([BSI 2006] S,122).
Die qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die digitale Signaturen nutzt, welche unter Verwendung von qualifizierten Zertifikaten und sicheren Signaturerstellungseinheiten erzeugt wurden ([BSI 2006] S,9).
Zertifikate sind nach §2 SigG *„elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird“*. Zudem existiert das qualifizierte Zertifikat, an welches erhöhte Anforderungen gestellt werden. Das qualifizierte Zertifikat wird von einem Zertifizierungsdiensteanbieter (ZDA) bereitgestellt. Dieser hat als vertrauenswürdige Instanz die Aufgabe, den Signaturschlüssel-Inhabern ihre Signaturschlüssel zuzuordnen. Der ZDA garantiert zudem, dass er die Anforderungen des SigG und der SigV gegenüber seiner Organisation erfüllt und die Angaben seiner Verzeichnis- und Zeitstempeldienste korrekt sind. Er sichert weiterhin die Korrektheit der Angaben in seinen qualifzierten Zertifikaten zu. Zu den Gesetzesforderungen gehört unter anderem der Betrieb der Zertifizierungsdienste in einer besonders geschützten Umgebung. Auch unterliegt die Aufklärung des Anwenders, im Hinblick auf seine Sorgfaltspflichten im Umgang mit der Signatur, dem ZDA ([BSI 2010]). Ein ZDA muss seinen Betrieb der zuständigen Behörde, der Bundesnetzagentur, mindestens anzeigen. Zusätzlich kann er sich auch akkreditieren lassen, was mit zusätzlichen Pflichten einhergeht, beispielsweise der Prüfung des Sicherheitskonzeptes des ZDAs. Er gewinnt dabei allerdings auch Vorteile, er erhält ein Gütesiegel der Bundesnetzagentur für sein geprüftes Sicherheitskonzept, des Weiteren stellt die Bundesnetzagentur dem akkreditierten ZDA auch seine Zertifikate aus ([BSI 2006] S,12).
Sichere Signaturerstellungseinheiten (SSEE) sind nach §2 Nr. 10 SigG *„Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind“*. SSEEs sollen dazu dienen, Signaturschlüssel zu speichern und die Erzeugung von qualifizierten elektronischen Signaturen zu ermöglichen.

Zudem sollen SSEEs Fälschungen der Signaturen verhindern, sowie Verfälschungen der Daten sichtbar machen und die Nutzung der Signaturschlüssel durch Unberechtigte verhindern. Aufgrund dieser Anforderungen darf es auch einem Signaturschlüsselinhaber nicht möglich sein, seinen privaten Schlüssel aus der Signaturerstellungseinheit auszulesen, da dies die Nichtabstreitbarkeit gefährden würde. Dass eine SSEE die Anforderungen erfüllt, muss durch eine Prüfung nach international annerkannten Sicherheitskriterien ([ITSEC] E3 hoch, [CC] EAL4+) und durch eine Überprüfung gemäß SigG nachgewiesen werden ([BSI 2006] S,133).
In §126 Absatz 3 des bürgerlichen Gesetzbuches (BGB, [Bund 2010b]) wird die Aussage getroffen, dass die Schriftform durch die elektronische ersetzt werden könne, so sich nicht aus dem Gesetz ein anderes ergäbe. Nach §371a der Zivilprozessordnung (ZPO, [Bund 2010c]) besitzen Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, denselben Stellenwert wie schriftlich signierte Dokumente (Urkunden). Vor diesem Hintergrund ist nur die qualifizierte elektronische Signatur in der Lage, die Papierdokumentation in rechtlicher Hinsicht gleichwertig zu ersetzen.

2.4.2 Technik

Die Erstellung einer elektronischen Signatur selbst ist ein rein technischer Vorgang. Für diesen Vorgang werden etablierte und als sicher erachtete Verfahren der Kryptologie verwendet.
Zur Signierung von Dokumenten werden in der Regel asymmetrische Kryptoalgorithmen verwendet. Diese beruhen auf der Verwendung eines privaten (Private Key) und eines öffentlich Schlüssels (Public Key) ([BSI 2006 S,21]). Der Grundgedanke ist es, die Signatur nur durch den Signaturschlüsselinhaber erstellen lassen zu können, welcher im Besitz des Private Key ist, sie jedoch durch jedwede Person verifizieren lassen zu können. Der Signaturschlüsselinhaber bedient sich zur Erstellung der Signatur einer Signaturtransformation, mit der er unter Nutzung seines privaten Schlüssels und der zu signierenden Nachricht die Signatur berechnet ([DIG 2001] Chapter 01 S,22). Der Empfänger kann unter zu Hilfenahme der Verifikationsfunktion anhand von Nachricht, Signatur und des öffentlichen Schlüssels bestimmen, ob die Nachricht durch den Signaturschlüsselinhaber erstellt wurde (Abbildung 12). Die beiden Schlüssel sind dabei so verknüpft, dass es mit ihnen möglich ist, Signaturen zu prüfen. Der Public Key wird dabei aus dem Private Key durch eine Einwegfunktion berechnet. Einwegfunktionen sind Funktionen, welche sich einfach berechnen, jedoch nur unter sehr hohem Rechenaufwand invertieren lassen. Dies verhindert, dass Angreifer aus dem öffentlichen Schlüssel den privaten Schlüssel berechnen können ([BSI 2006] S,21).

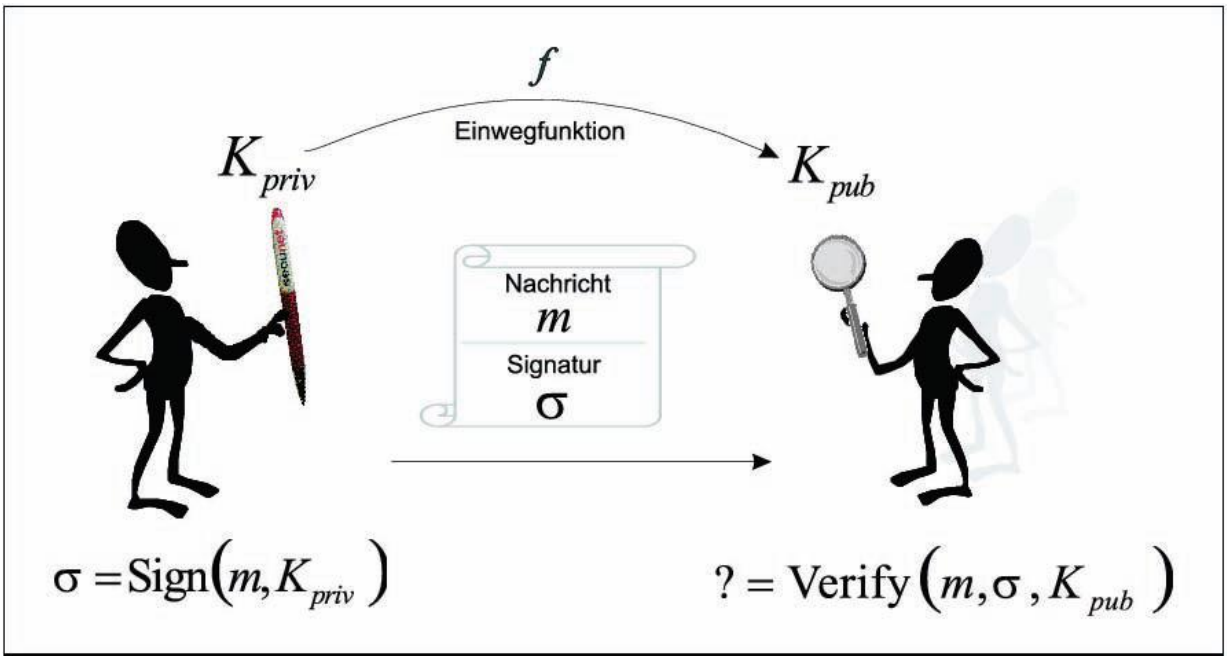

Abbildung 12: Prinzip der digitalen Signatur aus [BSI 2006] S,22

Um den privaten Schlüssel eines Schlüsselpaares sicher zu speichern, eignen sich Smartcards ([PKCS 2004] S,13). SSEEs können diese auslesen. Durch den Einsatz einer SSEE bleiben sensitive Informationen unzugänglich und werden nicht an die beteiligte Applikation weitergegeben. Durch den vermehrten Einsatz dieser Technologie ist es nötig, ein standardisiertes Interface für SSEEs anzubieten. Public Key Cryptography Standards (PKCS) #11 soll hier Abhilfe schaffen.
Eines der Ziele von PKCS #11 ist es, eine Zwischenschicht zwischen Applikation und dem Kartenlesegerät zu schaffen. Der Vorteil einer solchen Implementierung ist es, dass es für die Applikation unerheblich wird, was für ein Gerät tatsächlich benutzt wird, da die Applikation nur noch auf das Interface von PKCS #11 zugreift, welches den Zugriff auf das Kartenlesegerät regelt ([PKCS 2004 S,14]). PKCS bietet die Möglichkeit durch Bibliotheken dynamisch auf ein sich änderndes Umfeld zu reagieren und so entsprechend viele unterschiedliche Typen von Lesegeräten und Speicherformen von Informationen auf diesen Geräten anzusprechen. Der Nachteil dieses Ansatzes ist allerdings, dass es möglich ist, Bibliotheken einzuschleusen, welche die PIN des Benutzers abfangen könnten ([PKCS 2004 S,15]).
PKCS betrachtet Information, die auf Karten gespeichert sind als sogenannte Tokens. Aufgrund der verschiedenen Implementierungen diverser Hersteller legt PKCS die gespeicherten Informationen auf ein standardisiertes Objekt-Modell um. Zu den gespeicherten Daten können unter anderem Daten, Zertifikate und Schlüssel gehören. PKCS bietet dabei

ebenso eine Emulierung der diversen Funktionen, die ein Token bieten kann, auf ein standardisiertes Interface an ([PKCS 2004] S,15).
Die Nutzung von PKCS bietet eine Möglichkeit, Signaturen unabhängig von der verwendeten Hardware zu erstellen und somit auch längerfristig, ohne die Implementierung ändern zu müssen, einer Applikation Zugriff auf eine SSEE zu bieten.
Um PDF Dateien zu signieren gibt es entsprechende Implementierungen. Einzig sei hier hervorgehoben, dass sich aufgrund der geforderten langen Lesbarkeit von Einwilligungserklärungen besonders das PDF/A Format eignet. Zum einen, da das Dokument in sich vollständig sein muss, zum anderen, da es möglich ist gescannte Dokumente durch Optical character recognition (OCR) Texterkennung maschinenlesbar zu machen. Dies kann im Falle einer ausgedruckten und eingescannten Einwilligungserklärung nützlich sein ([PDFA 2010]).
XML Dokumente bieten eine große Flexibilität hinsichtlicher der Signierung. Es ist möglich das Dokument in einer Signatur zu verpacken, die Signatur dem Dokument als Element hinzuzufügen oder sie unabhängig vom signierten Dokument in einem eigenen Dokument festzuhalten ([BSI 2006] S,76). Zusätzlich ist es möglich nur bestimmte Teile des Markups in die Berechnung der Signatur einzubeziehen und andere gänzlich nicht zu beachten. Die Signatur besteht dabei ebenso aus Markup. Grundlegende Elemente einer XML Signatur sind folgende ([BSI 2006] S,77):

```
<Signature ID>
     <SignedInfo>
           <CanonicalizationMethod/>
           <SignatureMethod/>
           <Reference URI>
                   <Transforms>
                   <DigestMethod>
                   <DigestValue>
           </Reference>
     </SignedInfo>
     <SignatureValue>
     <KeyInfo>
     <Object ID>
</Signature>
```

Abbildung 13: Struktur einer XML-Signatur aus [BSI 2006] S,77

Die einzelnen Elemente beinhalten dabei folgende Informationen:

CanonicalizationMethod - beschreibt die Kanonisierungsmethode.

SignatureMethod - Informationen über den Signaturalgorithmus.

Reference - Kann einen Verweis auf die zu signierenden Daten enthalten. Hierfür wird ein Uniform Resource Identifier (URI) genutzt.

Transforms - Informationen über die Art der Aufbereitung vor Nutzung der Hashfunktion.

DigestMethod - Spezifizikation der anzuwendenden Hashfunktion.

DigestValue - Hashwert der durch Anwendung der Hashfunktion berechnet wurde.

SignatureValue - Die eigentliche Signatur.

KeyInfo - Element, das beispielsweise zur Ablage von Zertfikaten benutzt werden kann.

Object - Element für beliebige Daten.

2.5 Lösungsansätze zur Erstellung von Einwilligungserklärungen

Es wurde bereits versucht ein Einwilligungsmanagement elektronisch zu realisieren. Es soll daher ein kurzer Überblick über diese Ansätze gegeben werden, da sie aufzeigen, welche Probleme bei der Entwicklung eines Einwilligungsmanagements auftreten können.

2.5.1 Technische Universität Ankara

2006 veröffentlichten Namli und Dogac ein an der technischen Universität Ankara entwickeltes Konzept eines Einwilligungsmanagements basierend auf BPPC und XACML ([Namli und Dogac 2006]). Dieses Konzept basiert auf einem System in dem die Zugriffsentscheidung durch Einbeziehen der Rolle des anfragenden Benutzers und des PolicySets des Patienten getroffen wird. Der Patient kann dabei über einen sogenannten Consent Editor die Einstellungen seiner Einwilligungserklärung ändern und nach seinen Wünschen anpassen. Der Consent Editor bietet dazu die Möglichkeit zwischen drei Konfigurationsmodi zu wählen. Im Basismodus kann der Patient lediglich rudimentäre Einstellungen vornehmen, beispielsweise an welche Personengruppen seine Daten weitergegeben werden dürfen oder ob der Patient selbst seine Daten einsehen darf. Im Modus für fortgeschrittene Benutzer ist es den Benutzern möglich mit feinerer Granularität festzulegen, welche Personengruppe auf welche Dokumententypen zugreifen darf. Beispielhaft für die Personengruppen seien hier Ärzte oder das administrative Personal genannt. Die Dokumententypen sind beispielsweise administrativer oder medizinischer Natur.

Der Expertenmodus bietet die Möglichkeit weitere Faktoren in die Konfiguration einzubeziehen, beispielsweise kann der Patient seine Einwilligung so einstellen, dass er über jeden Zugriff auf seine Akte informiert wird. Auch ist es möglich den Zugriff nach Uhrzeit oder anderen Umweltfaktoren zu regeln.
Das Konzept von Namli bietet hierbei keine Möglichkeit den Zugriff gezielt für eine Einrichtung oder einen Arzt zu beschränken. Lediglich die Unterscheidung zwischen den Personengruppen, welche Zugriff erlangen möchten, ist möglich. Die Einstellungen auf Dokumentenebene lassen keine Konfiguration für einzelne Dokumente oder bestimmte medizinische Dokumentengruppen, beispielsweise Arztbriefe zu. Unterschieden werden medizinische Dokumente lediglich in den Kategorien Diätanweisungen, allgemeine klinische Informationen, sensitive klinische Informationen, Angaben zur Medikation und Informationen zur Forschung. Es ist nicht ersichtlich, in welche Kategorien einzelne Dokumente, beispielsweise Röntgenbilder, fallen.
Namli beschreibt den Ablauf der angestrebten Verarbeitung seiner PolicySets so, das der Verarbeitungsalgorithmus only-one-applicable genutzt wird. Ob die Erzeugung der PolicySets dieses Ansatzes dynamisch erfolgt lässt sich aus der Veröffentlichung nicht erfahren. Es wird lediglich beschrieben, dass der Patient aus „Privacy Consent Policies“ auswählen könne, jedoch nur eine wählen sollte, da diese möglicherweise gegensätzliche Bestimmungen enthalten. Dies legt vordefinierte PolicySets nahe, es kann aber keine definitive Aussage getroffen werden.
Unklar is daher auch, was geschieht wenn eine neue Einrichtung der einrichtungsübergreifenden Patientenakte beitritt. Eine vorgefertigte Einwilligungserklärung müsste möglicherweise aufwändig aktualisiert werden.
Namlis Ansatz bietet zudem keine Möglichkeit der Signatur. Die Vornahme der Einstellungen erfolgt rein elektronisch, die Einwilligungserklärung wird jedoch weder schriftlich festgehalten, noch mit einer elektronischen Signatur versehen.

2.5.2 Elektronische Fallakte (eFA)

Ein weiterer Ansatz zur Realisierung eines Einwilligungsmanagements wurde durch [Caumanns 2008] erarbeitet. Die sogenannte elektronische Fallakte (eFA) beschreibt wie die Bestimmungen der Einwilligungserklärungen der Patienten innerhalb eines Netzwerkes umgesetzt werden sollen. Die eFA unterscheidet sich dabei grundsätzlich vom Ansatz des intersektoralen Informationssystems. Während letzteres eine komplette Historie der Dokumente eines Patienten aufbaut, hat die eFA zum Ziel, lediglich für einen konkreten Fall benötigte Daten zur Verfügung zu stellen. Die Daten bleiben dabei dezentral in den Systemen der Leistungserbringer gespeichert und werden den zugreifenden Personen zur Verfügung gestellt.

Die Regelung des Zugriffes auf die Daten erfolgt dabei unter der Verwendung mehrerer Schritte zur Authentifizierung des Benutzers. Erst nach der Authentifizierung, Zuweisung einer Rolle und mehrfacher Absicherung dieser Informationen durch zusätzliche Authentifizierung kann der Benutzer versuchen auf eine Fallakte zuzugreifen. Durch Wahl der Fallakte sendet der Client die OID der Akte an den Access Token Service, welcher die bestehenden Authentifizierungsinformationen an einen Policy Administration Point (PAP) weiterleitet. Dort wird dann die Policy des Patienten ausgewertet, welche den Zugriff beschränken soll. Sollte die Evaluation der Policy im PAP den Zugriff ermöglichen, wird dieser gewährt.
Die Authentifizierungsmaßnahmen dieses Ansatzes schließen Missbrauch nahezu komplett aus, der hohe Aufwand der Authentifizierung und die Komplexität der mehrfachen Authentifizierung stehen dem allerdings gegenüber. Zudem scheint die Integration in bestehende Systeme mit erheblichem Arbeitsaufwand verbunden.
Die, im Rahmen der eFA durch den Patienten abgegebene, Einwilligungserklärung wird, so wie im vorherigen Ansatz von Namli, durch XACML codiert. Caumanns trifft allerdings keine Aussage, wie die Polices des Patienten erstellt werden sollten. Zudem trifft er die Aussage, dass die erteilte Einwilligung immer für die gesamte Fallakte eines Patienten als Ganzes gelte und es einem, durch den Patienten festgelegten Personenkreis, ermögliche, übergreifend definierte Operationen auf seiner Fallakte auszuführen. Es scheint daher fraglich, ob es Patienten möglich ist, gezielt einzelne Vorgänge gemäß ihrer Wünsche zu verhindern oder einzelne Personen vom Zugriff auszuschließen.

2.5.3 Ideales Einwilligungsmanagement

Ausgehend von den zwei bisher beschriebenen Ansätzen entwickelte daher [Birkle 2009b] ein Konzept eines idealen Einwilligungsmanagements (IEM). Dieses Konzept sollte es ermöglichen, Zugriffsbeschränkungen auf sowohl Personen- als auch Dokumentenebene zu formulieren. Zudem sollten die Zugriffsberechtigunge lediglich das Erzeugen und Einsehen von Dokumenten beinhalten. Das Löschen von Dokumenten wurde nicht berücksichtigt, da dies einer Sperrung des Dokumentes im Quellsystem entspricht. Die Änderung von Dokumenten wurde ebenfalls vernachlässigt, da dies zu einem neuen Dokumenteneintrag im eEPA-System führt.

Das Konzept des IEM geht, aufgrund der gesetzlichen Rahmenbedingungen, von einer Opt-In Lösung aus. Ausgehend von der Forderung, Zugriffsberechtigungen auf Personen- und Dokumentenebene festlegen zu können, wurde eine n*n Matrix für die Beziehungen zwischen den einzelnen Akteuren und den verfügbaren Dokumenten entwickelt. Innerhalb dieser n*n Matrix können für die Schnittstellen zwischen den Dokumenten und den Akteuren die Berechtigungen Lesen und Erzeugen eingestellt werden. Dies ermöglicht es beispielsweise, einzelnen Akteuren das Einstellen bestimmter Dokumente zu untersagen.

Die angestrebte n*n Matrix bietet zwar sehr differenzierte Möglichkeiten zur Festlegung der Berechtigungen, allerdings ist die Größe der Matrix das Problem dieses Ansatzes. Die Matrix würde für eine große Anzahl an teilnehmenden Einrichtungen und Dokumenten sehr schnell nicht mehr überschaubar. Die Verarbeitung würde zudem immer langsamer werden.
Die Verwaltung der Matrix scheint zudem nicht realisierbar. Die schiere Größe und die Möglichkeiten, die Einstellungen anzupassen, würden sich durch einen durchschnittlichen Benutzer wohl nicht überschauen lassen.

3 Methoden und Werkzeuge

Zu den initalen Vorgaben des Auftraggebers gehörte, aufgrund der bisher gemachten Erfahrungen, die Verwendung der in Kapitel 2 beschriebenen Technologien und Standards als Grundlage der Implementierung. Diese sollten die Basis des Webservices bilden.
Um die Anforderungen an den zu erstellenden Webservice zu erfassen wurden die Experten der Leitung des ISIS Projektes befragt. Diese Befragung wurde nach dem Prinzip der persönlichen Befragung durchgeführt. Die Experten wurden im Hinblick auf ihre funktionalen Anforderungen an den Webservice befragt, welche Technologien und Standards sie in die Entwicklung des Webservices einbeziehen würden und wie der Webservice sich in die Systemlandschaft der künftigen Anwendungsumgebung eingliedern sollte. Die festgestellten Anforderungen wurden zunächst schriftlich festgehalten. Zu der Feststellung der zu implementierenden Funktionalitäten gehörte auch die Feststellung der zu erwartenden Benutzergruppen. Diese wurden ebenfalls durch die persönliche Befragung der Experten erfasst.
Ausgehend von der schriftlichen Feststellung der geforderten Funktionalitäten für die einzelnen Benutzergruppen wurden diese Funktionen in einem Unified Modelling Language[10] Use Case-Diagramm modelliert. Die Modellierung wurde unter Zuhilfenahme des UML-Modellierungstools Visual Paradigm[11] bewerkstelligt. Der Modellierungsvorgang ist Teil der objektorientierten Analyse mittels derer die Anforderungen an das System erfasst und beschrieben werden sollen. Dieses Diagramm beinhaltet die festgestellte Funktionalität und deren Bezug zu den jeweiligen Benutzern. Das Diagramm wurde den Experten wiederholt vorgelegt bis alle Anforderungen, die initial in den Gesprächen nicht erfasst wurden, berücksichtigt wurden. Der Ablauf dieser Entwicklung entspricht der Entwicklung unter Verwendung eines Wasserfallmodells mit Rücksprungmöglichkeiten.
Nach Abschluss dieser Phase wurden die Anforderungen an die zu erstellende Einwilligungserklärung mit den Experten besprochen und in Einklang mit den erarbeiteten rechtlichen Rahmenbedingungen und im Hinblick auf die zu verwendende elektronische Signatur angepasst und schließlich schriftlich festgehalten.
Ebenso wurden die konkreten Anforderungen an die Implementierung des Webservices aus den bereits festgestellten Anforderungen der Experten abstrahiert und diesen zur Kontrolle vorgelegt.
Auf Basis der kompletten Anforderungen wurden die festgestellten Use Cases schriftlich in der Gesamtheit ihres Ablaufes und ihrer möglichen Alternativabläufe ausformuliert und erneut den Experten vorgelegt.
Nach der Feststellung aller benötigten Funktionen und der Anforderungen an den Webservice sowie an die zu erstellende Einwilligungserklärung und unter Berücksichtigung der

[10] *http://www.uml.org*
[11] *http://www.visual-paradigm.com/*

künftigen Anwendungsumgebung wurde ein Konzept für die Einwilligungserklärung und deren Repräsentation in menschen- und maschinenlesbarer Form entwickelt.
Nach Abschluss dieser Phase wurde ein UML Klassendiagramm mittels Visual Paradigm entwickelt. Auf Basis dieses Diagrammes wurden UML Sequenzdiagramme der Use Cases in Visual Paradigm modelliert, welche wiederum den Experten vorgelegt wurden.

Für die Wahl der Technologien zur Implementierung des Consent Creators wurden sowohl die, in der Anforderungsanalyse festgestellten, funktionalen als auch technischen Anforderungen einbezogen. Zudem wurde darauf geachtet, das entwickelte Konzept der Einwilligungserklärungen mit den gewählten Technologien umsetzen zu können.
Um die in der Anforderungsanalyse festgestellten Systemanforderungen an den Consent Creator umzusetzen fiel die Wahl der Technologie für die Oberfläche zunächst auf ExtJS[12], eine Javascript Bibliothek. ExtJS ermöglicht die Darstellung von fortgeschrittenen Komponenten, beispielsweise Baumstrukturen, ohne auf Anwenderseite eine Installation von Software zu erfordern. Es wurde zunächst ein Prototyp in ExtJS entwickelt, welcher anschließend mit geringer Funktionalität ausgestattet wurde. Im Zuge der Präsentation dieses Prototyps stellte der ISIS-Betreiber allerdings fest, dass die Lizenz unter der ExtJS verfügbar ist, nicht mit den Zielen des Betreibers vereinbar ist. Entsprechend musste die Entwicklung einer Oberfläche auf Basis von ExtJS verworfen werden. Infolge dessen wurde nach Alternativen gesucht und die Umsetzbarkeit einer Oberfläche mit JavaFX[13] analysiert. Da die Analyse von JavaFX jedoch zu Tage brachte, dass die Umsetzung mit dieser Technologie nicht den Anforderungen des Betreibers entsprechen würde, wurde dieser Ansatz ebenfalls verworfen.
Die Wahl fiel letztlich auf eine Umsetzung der Oberfläche mittels HTML und CSS. Da diese Technologien jedoch keine Baumstrukturen bieten, welche für die Darstellung der an ISIS teilnehmenden Organisationen zur Erstellung einer Einwilligungserklärung benötigt werden, wurde beschlossen diesen Teil der Oberfläche in einem Java Applet umzusetzen.
Die Anforderungen im Hinblick auf die elektronische Signatur der Einwilligungserklärungen bedingten ebenso die Wahl eines Java Applets für die Funktionalität der Signatur.
In Gesprächen mit den Experten des ISIS Projektes wurde zudem festgestellt, dass bereits für das Teleradiologie Webportal ([Schneider 2010]) des Universitätsklinikums Heidelberg ein CSS-Layout des Corporate Designs des Universitätsklinikums erstellt wurde. Dieses wurde nach Abstimmung mit den Experten für die Erstellung der Oberfläche genutzt und in wenigen Punkten an die Anforderungen an den Consent Creator angepasst.
Die Implementierung des Webservices wurde aufgrund der bisher gemachten Erfahrungen mittles einer Model 2 Architektur realisiert.
Die Antworten des Consent Creators auf Anfragen enthalten, um ein einfaches Austau-

[12] *http://www.sencha.com/products/js/*
[13] *http://javafx.com/*

schen der Oberfläche zu ermöglichen, nur einfache Textbausteine. In Fällen in denen größere Mengen an Daten zurückgegeben werden müssen, beispielsweise Listen, werden diese Daten mittels JSON[14] strukturiert und zurück geschrieben. JSON ist ein Datenformat für den Austausch von menschenlesbaren Informationen, ähnlich XML. JSON bietet jedoch aufgrund der Reduzierung des Markups auf minimale Strukturen den Vorteil gegenüber XML, geringeren Datenoverhead zu erzeugen. Dies ist insbesondere bei der Transferierung von großen, strukturierten Daten, beispielsweise Listen, über ein Netzwerk mit beschränkter Bandbreite von Vorteil.
Als Applikationsserver wurden sowohl Glassfish[15] als auch Apache Tomcat[16] in Erwägung gezogen. Die Wahl des Applikationsservers für den Consent Creator fiel aufgrund der Systemlandschaft des ISIS Betreibers auf Apache Tomcat, entsprechend wurde die Implementierung des CC in Java geschrieben.
Die Datenbank wurde, um SQL Injections zu vermeiden, mittels Prepared Statements implementiert. Die Datenbank selbst greift dabei auf eine Connection Factory zu, welche mittels Proxool[17] die Verbindung zur Datenbank aufbaut. Proxool dient dazu, die Wahl der Datenbank und des Datenbank Connectors einfach über eine Konfigurationsdatei austauschen zu können.
Die Forderungen an das Format der Einwilligungserklärung in ihrer maschinenlesbaren Form wurden mittels eines an den BPPC Standard angelehnten CDA Dokumentes gelöst. Der BPPC Standard enthält bereits die benötigten Strukturen um die Daten des Patienten und die der, im rechtlichen Rahmen an der Erstellung der Einwilligungserklärung beteiligten, Personen festzuhalten. Das XML Format des CDA Dokumentes eignet sich auch um den rechtlich verbindlichen Text zu speichern, der für die Generierung der menschenlesbaren Version der Einwilligungserklärung benötigt wird. Die Speicherung des rechtlich verbindlichen Textes im CDA Dokument erfüllt zudem die Anforderung der Vollständigkeit an die elektronische Signatur. Es wurde für die Speicherung des Textes innerhalb eines section Elementes des CDA Dokumentes entsprechende Strukturen angelegt. Das maschinelllesbare Format wird mittels XSL-FO[18] in eine menschenlesbare Darstellung transformiert, welche im PDF Format gespeichert wird. Aus Gründen der Vollständigkeit wird auch dieses Dokument, in einer Base64 transformierten Version, im CDA Dokument vorgehalten. Da das CDA Dokument alle relevanten Informationen enthält und sich die menschenlesbare Form daraus jederzeit wieder herstellen lässt, wird lediglich dieses Dokument mit einer qualifizierten elektronischen Signatur versehen.
Die Schnittstellen zu den anderen Teilsystemen des intersektoralen Informationssystems

[14] *http://www.json.org/*
[15] *https://glassfish.dev.java.net/*
[16] *http://tomcat.apache.org/*
[17] *http://proxool.sourceforge.net/*
[18] *http://www.w3.org/TR/xsl/#fo-section*

wurden mittels HL7 realisiert. Dies geschah im Hinblick auf die Standardkonformität und Interoperabilität des Consent Creators, eigene Lösungen die keine Interoperabilität mit neuen Teilsystemen ermöglichen würden wurden damit hinfällig. Die für die Kommunikation mit den anderen Teilsystemen benötigten Nachrichten wurden entsprechend vereinbart und dokumentiert.
Als Entwicklungsumgebung für die Implementierung wurde aufgrund bisher gemachter Erfahrungen Eclipse[19] gewählt. Die Implementierung wurde abschließend systematisch durch JUnit-Tests[20] getestet. JUnit-Tests wurden im Hinblick auf die Reproduzierbarkeit der Ergebnisse der Tests gewählt. Die Oberfläche wurde entsprechend der ausformulierten Use Cases systematisch getestet.

[19] *http://www.eclipse.org/*
[20] *http://www.junit.org*

4 Anforderungsanalyse

Wie im vorherigen Kapitel beschrieben wurden die Anforderungen an den Webservice durch die Befragung der Experten des ISIS Projektes festgestellt. Die schriftliche Darlegung der Ergebnisse dieser Befragung befindet sich in diesem Kapitel. Das Use Case Diagramm, welches die konkreten Funktionen illustriert, die den Benutzern zur Verfügung stehen, befindet sich in Anhang B.1. Dort befinden sich auch die konkreten Formulierungen der Abläufe und Alternativabläufe der Use Cases.

4.1 Funktionalität

Zu den zentralen Anforderungen an die Funktionalität des Consent Creator (CC) gehört es, eine Möglichkeit zur Erstellung einer Einwilligungserklärung für einen Patienten bereitzustellen. Um eine Einwilligungserklärung zu erstellen, muss es der CC dem Patienten ermöglichen, seine Vorgaben im Hinblick auf den Zugriff auf seine Daten in einer maschinell verarbeitbaren Form festzuhalten. Der Patient muss hierfür die Möglichkeit erhalten, aus den an ISIS beteiligten Organisationen und Personen auswählen zu können und ihnen den Zugriff auf seine Dokumente zu ermöglichen oder zu verwehren. Darüber hinaus muss der CC in der Lage sein, eine menschenlesbare Präsentation dieser Vorgaben zu erzeugen und diese dem Patienten anzeigen zu lassen. Aus diesen Vorgaben lassen sich Datenschutzregeln ableiten, welche dazu genutzt werden können, den Zugriff auf seine Dokumente entsprechend der Wünsche des Patienten zu beschränken. Der Zugriff auf die Einwilligungserklärung des Patienten muss ihm selbst und dem klinischen Personal vorbehalten sein. Es ist daher erforderlich nur authentifizierten Zugriff auf den CC zuzulassen und diese Zugriffe zu protokollieren. Der CC muss hierfür eine Benutzerverwaltung bereitstellen, in der Patienten sich selbst registrieren oder durch den Leistungserbringer hinzugefügt werden können. Zugriffe aus dem KIS-Kontext sollten grundsätzlich erlaubt sein. Teil der Benutzerverwaltung muss auch sein, bereits vorhandene ISIS Patientenprofile mit neu angelegten Patientenprofilen im CC zu verknüpfen. Die entsprechenden Patientenprofile müssen dann durch den ISIS-Betreiber allerdings aus Sicherheitsgründen freigeschaltet werden. Dies darf jedoch erst erfolgen, wenn sichergestellt ist, dass es sich bei der anmeldenden Person auch um den Patienten selbst handelt.
Die Einwilligungserklärung ist durch die rechtlichen Rahmenbedingungen ohne Unterschrift oder qualifizierte elektronische Signatur nicht gültig. Der CC muss es ermöglichen, entweder die gescannte und unterschriebene Einwilligungserklärung dem maschinell lesbaren Format hinzuzufügen, oder die Einwilligungserklärung mit einer qualifizierten elektronischen Signatur (Siehe Kapitel 2.4.1) zu versehen. Die Rechtslage bedingt zudem die Archivierung der Einwilligungserklärung. Der CC benötigt hierfür Schnittstellen zum Consent Manager (siehe Glossar - Anhang A). Schnittstellen zum CM werden auch benötigt um die aus den

Vorghaben des Patienten abgeleiteten Datenschutzregeln zu versenden und die erstellten Dokumente für die Benutzer über den CC zur Ansicht zugänglich zu machen. Zudem werden auch Schnittstellen zu PORS, VPA und MPI benötigt (Siehe Kapitel 2.1). Von PORS werden Informationen über die an ISIS beteiligten Organisationen bezogen. VPA muss es ermöglichen eine Liste aller Dokumente eines Patienten zu beziehen. Der MPI muss es ermöglichen Patienten anlegen zu können, um die im CC gespeicherten Profile mit ISIS zu verknüpfen. Ebenso muss der CC in der Lage sein von den Primärsystemen der Leistungserbringer gesendete Informationen zu verarbeiten. Dies wird für die Anmeldung des Personals der Leistungserbringer benötigt. Benötigt werden auch Funktionen um es dem Patienten zu ermöglichen, seine Einwilligungserklärung zurückzuziehen und dadurch den Zugriff auf seine Dokumente zu sperren, sowie die Möglichkeit die Teilnahme an ISIS zu beenden. Der Leistungserbringer benötigt ebenso eine Funktionalität um Teilnehmer zu inaktivieren, so wie er diese auch wieder aktivieren können muss. Dem Leistungserbringer muss es auch möglich sein die Einwilligungshistorie eines Patienten einsehen zu können, um im Falle eines Rechtsstreits belegen zu können, wann welche Datenschutzregeln in Kraft waren. Benutzer müssen zusätzlich noch in der Lage sein, ihr Passwort wiederzuerlangen, sollten sie dieses vergessen haben. Um die Daten der Benutzer aktuell zu halten und etwa Adressänderungen zu berücksichtigen muss es möglich sein die Daten der Benutzer zu editieren, so wie diese selbst ihre Daten in begrenzterem Umfang auch editieren können sollten.

4.2 Einwilligungserklärung

Die Einwilligungserklärung des Patienten muss sowohl in einer maschinell-, als auch menschenlesbaren, Version verfügbar sein. In ihr müssen Informationen über den Patienten, den Autor der Einwilligungserklärung und weitere vom BPPC Profil genannte Akteure gespeichert werden. Die, durch BPPC identifizierten, Akteure müssen mit den Informationen zu an ISIS beteiligten Personen abgeglichen werden. Durch diesen Abgleich wird ersichtlich, wessen Daten in den entsprechenden Datenfeldern der Akteure des BPPC Profils gespeichert werden müssen. Interoperabilität der Einwilligungserklärung muss gewährleistet werden, um später mit zum Zeitpunkt dieser Arbeit noch nicht etablierten Systemen einwandfrei kommunizieren zu können.
Aufgrund der Forderung der Vollständigkeit der elektronischen Signatur müssen sowohl die menschenlesbare als auch die maschinelle Formulierung der Datenschutzregeln in dem zu archivierenden Format untergebracht werden. Ebenso sollte der für die Erstellung der Einwilligungserklärung erforderliche rechtlich verbindliche Text in der Einwilligungserklärung präsent sein. Die Einwilligungserklärung muss entsprechend des jeweiligen Benutzers und der damit verbundenen Menge an Datenschutzregeln dynamisch erzeugt werden.
Rechtliche Rahmenbedingungen, die in [Birkle 2009a] erarbeitet wurden, müssen entspre-

chend berücksichtigt werden.
Die Einwilligungserklärung muss eindeutig zuzordnen sein, um Fehler bei der Durchsetzung der Datenschutzregeln ausschließen zu können.

4.3 Systemanforderungen

Der Consent Creator (CC) muss die ihm anvertrauten Daten effektiv schützen, dementsprechend muss das System den Zugriff Unbefugter verhindern. Hierfür ist es notwendig, sowohl SSL[21] zu implementieren als auch vor Ausführung von Anfragen zu prüfen, ob der Benutzer eingeloggt, seine Anfrage valide ist und er die benötigten Rechte besitzt. Des Weiteren muss die Ausführung von Schadcode auf der Datenbank verhindert werden. Um die Erweiterbarkeit des CCs zu ermöglichen, sollte dieser modular aufgebaut werden. Da der CC nicht nur am Universitätsklinikum Heidelberg eingesetzt werden soll, ist die leichte Austauschbarkeit der Komponenten und Konfigurationen des Systems mit in die Konzeption einzubeziehen. Die grafische Oberfläche sollte das Corporate Design des Universitätsklinikums Heidelberg umsetzen. Es sollte möglich sein, die grafische Oberfläche des CCs ohne großen Aufwand durch eine Implementierung Dritter ersetzen zu können. Hierfür ist es wichtig, das Design der Oberfläche entsprechend leicht anpassen zu können, ohne diese komplett neu schreiben zu müssen. Entsprechend sollte auch die Konfiguration der Datenbank leicht angepasst werden können, um nicht von einem Produkt eines Herstellers abhängig zu sein und die Betriebsumgebung und Produktwahl des jeweiligen Betreibers zu berücksichtigen. Das Konzept der Datenbank sollte zusätzlich eine einfache Erweiterbarkeit der Tabellenstruktur berücksichtigen.
Die Kommunikation des CC sollte sich an Standards orientieren um die Interoperabilität mit zukünftigen ISIS Teilsystemen zu ermöglichen. Es ist nötig die Kommunikation mit dem Consent Manager festzulegen, um später eindeutig einsehen zu können, welche Antworten bestimmte Nachrichten hervorrufen. Schnittstellen zu den ISIS Teilsystemen MPI, VPA und PORS werden ebenso benötigt. Die Darstellung der Interaktion der einzelnen Systeme befindet sich in Abbildung 14, Kapitel 5.1.
Das System des CC sollte zudem schnellen Zugriff ermöglichen um das Personal der Leistungserbringer nicht unnötig warten zu lassen und sie an ihrer Arbeit zu hindern. Es sollte daher bei der Technologiewahl darauf geachtet werden nur Technologien zu nutzen, welche schnelle Verfügbarkeit der Anwendung garantieren. Das System muss dem Benutzer auch für jede seiner Anfragen eine Rückmeldung über den Status der Anfrage beziehungsweise deren Ergebnis zukommen lassen. Die Abläufe der Anwendungsfälle sollten restriktiv sein und nur ein Minumum an Freiheiten erlauben, da es sonst zu nicht kontrollierbaren Abläufen kommen könnte, welche in dieser sensiblen Umgebung schwere Folgen haben könnten.

[21] *http://en.wikipedia.org/wiki/Transport_Layer_Security*

5 Konzept

Ausgehend von den Ergebnissen der Anforderungsanalyse soll in diesem Kapitel gezeigt werden, wie das entwickelte Konzept diese erfüllt. Das Konzept zur elektronischen Speicherung der Einwilligungserklärungen soll dabei verdeutlichen, wie diese erzeugt und verarbeitet werden, um die Vorgaben des Patienten zu erfüllen, welche in seiner Einwilligungserklärung festgehalten werden.

Der CC stellt die, in der Anforderungsanalyse geforderten, Funktionen zur Erzeugung von Einwilligungserklärungen zur Verfügung. Der Patient/Leistungserbringer kann sich im CC anmelden und eine Einwilligungserklärung erzeugen. Dies geschieht durch die Erstellung von Datenschutzregeln (Siehe Glossar - Anhang A), welche in einem PolicySet (Siehe Glossar - Anhang A) festgehalten werden. Sollte der Patient mit seinen Datenschutzregeln zufrieden sein und diese speichern wollen, wird aus dem PolicySet und dem CDA Dokument, welches angelehnt an das BPPC Profil ist und unter anderem die Textpräsentation der Basiseinwilligung enthält, eine Repräsentation der Einwilligung als PDF generiert. Der Patient erhält diese Präsentation zur Ansicht und kann dann entscheiden, ob er diese Einwilligung akzeptieren will. Sollte der Patient zufrieden sein, signiert er die Einwilligungserklärung und speichert diese. Das CDA Dokument wird dann mit dem enthaltenen PolicySet und generierten PDF an den Consent Manager (Siehe Glossar - Anhang A) gesendet.
Die Interaktion des Consent Creators mit ISIS-Teilsystemen wird in Abbildung 14 illustriert.

Das PolicySet wird aus Datenschutzregeln konstruiert, welche der Patient selbst zusammenstellen kann, bsp: <Organisation> <Dokument> <Zugriff verbieten> oder <Organisation> <Krankenschwestern> <Bluttests> <Zugriff verbieten>.
Grundlegende Informationen einer Datenschutzregel sind:
Informationen über die von der Datenschutzregel betroffenen Personen.
Informationen über die von der Datenschutzregel betroffenen Dokumente.
Informationen über die Art der Aktion, die auf den betroffenen Dokumenten ausgeführt werden soll. Im Normalfall sind dies Lese- oder Schreibvorgänge.

Diese Regeln werden dann in menschenlesbarer Form formuliert, um sie in der Einwilligungserklärung anzuzeigen und es dem Patienten zu ermöglichen, abschätzen zu können, welche Folgen sein Handeln hat. Die Formulierungen der Datenschutzregeln müssen so gewählt werden, dass sie eindeutig und rechtssicher sind.
Die Liste der Organisationen, aus denen ein Patient wählen kann, wird dabei aus PORS abgefragt. Dieser Vorgang muss nicht zwingend bei jedem Aufruf des CC geschehen, son-

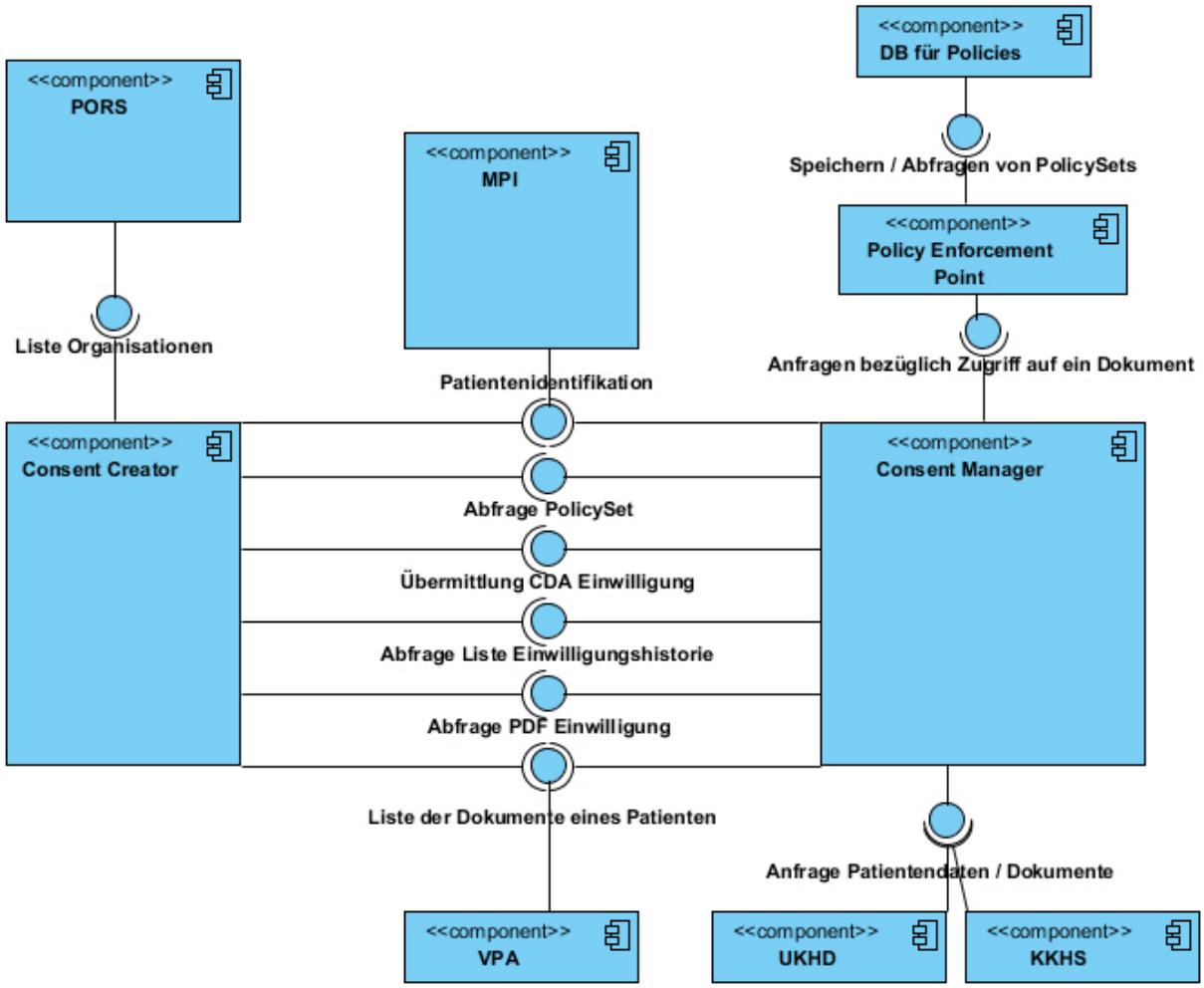

Abbildung 14: Darstellung der Interkationen des Consent Creator

dern kann einmal pro Woche erfolgen, da die Fluktuation der Organisationen als gering angenommen werden kann. Alternativ könnte ein Update von Seiten PORS erzwungen werden. In beiden Fällen werden entsprechende Listen der Organisationen im CC vorgehalten werden.
Der Patient benötigt zur Formulierung der Datenschutzregeln auch eine komplette Liste seiner in ISIS vorgehaltenen Dokumente. Diese Liste muss dynamisch von der VPA abgefragt werden, da hier aktuelle Informationen benötigt werden, um nahtlosen und schnellen Informationsaustausch zu gewährleisten, beispielsweise für Nachsorgetermine beim Hausarzt eines Patienten kurz nach einer Operation. Ebenso kann durch das Betrachten der Dokumente durch den Patienten entschieden werden, welche Dokumente er freigeben oder sperren möchte. Sollte es nicht möglich sein die benötigten Dokumente zeitnah freizugeben, würde dies den Nutzen von ISIS entscheidend mindern. Initial besitzt der Patient im

ISIS System keine Dokumente. Dies liegt darin begründet, dass Dokumente erst nach einer Erklärung der Teilnahme an ISIS in das System eingestellt werden.
Das Login des CC muss es sowohl dem Patienten als auch dem Organisationspersonal ermöglichen sich einzuloggen. Im Falle der Patienten ist es notwendig das genutzte Login einer Patienten-ID aus dem MPI eindeutig zuzuordnen, um die erzeugte Einwilligungserklärung dem richtigen Patienten zuordnen zu können.
Sollte eine Organisationseinheit bei ISIS Dokumente eines Patienten anfragen um diese anzusehen, so wird initial nach allen vorliegenden Dokumenten eines Patienten gefragt, um dem Anfragesteller eine Liste der Dokumente des Patienten anzuzeigen. Die Anfrage wird an den CM gestellt und enthält Informationen über die Person, welche anfragt, und ob alle Dokumente des Patienten angefragt werden. Der CM muss nun eine Liste aller Dokumente des Patienten von der VPA abfragen und prüfen, ob der Anfragesteller Zugriff auf die Dokumente erhalten darf. Hierfür ist es notwendig, für jedes Dokument aus der Liste eine Anfrage an den im CM integrierten, Policy Enforcement Point (PEP) zu stellen. Der PEP prüft, ob im PolicySet des Patienten eine Datenschutzregel vorhanden ist, welche dem Anfragesteller Zugriff auf das Dokument gewährt oder verwehrt. Sollte dies der Fall sein, so wird das Ergebnis dieser Datenschutzregel durch den PEP an den CM zurückgegeben. Sollte es keine Datenschutzregel für den Anfragesteller und das Dokument geben, so wird der Zugriff standardmäßig verwehrt. Dieser Vorgang wiederholt sich für alle Dokumente des Patienten. Der CM erstellt intern eine Liste der Dokumente, für die der Zugriff gewährt wurde. Abschliessend wird die Liste der Dokumente an den Anfragesteller zurückgegeben. Der Anfragesteller kann nun diese Dokumente einsehen. Eine erneute Überprüfung, ob der Anfragesteller diese Dokumente einsehen darf, ist beim Aufruf des Dokumentes nicht nötig, da er nur Informationen über Dokumente erhalten hat, welche er einsehen darf, dementsprechend kann er auch nur diese Dokumente anfordern.

Der CC muss in der Lage sein, Datenschutzregeln für folgende Anwendungsfälle erstellen zu können:

1) Organisation darf auf alle Dokumente eines Patienten zugreifen.

2) Organisation darf nur auf bestimmte Daten eines Patienten (nicht) zugreifen.

3) Organisation darf nur auf ein Dokument eines Patienten (nicht) zugreifen.

4) Organisation darf gar nicht auf Dokumente eines Patienten zugreifen.

5) Person(engruppe) darf auf alle Dokumente eines Patienten zugreifen.

6) Person(engruppe) darf nur auf bestimmte Daten eines Patienten (nicht) zugreifen.

7) Person(engruppe) darf nur auf ein Dokument eines Patienten (nicht) zugreifen.

8) Person(engruppe) darf gar nicht auf Dokumente eines Patienten zugreifen.

Beispiel einer Datenschutzregel für die Fälle 5-8 wäre die Beschränkung des Zugriffes für Ärzte einer Abteilung auf Dokumente, die in ihrer Abteilung erstellt wurden.
Mehrere Datenschutzregeln können auf eine Anfrage anwendbar sein, beispielsweise wenn eine Datenschutzregel den Zugriff auf ein bestimmtes Dokument verwehrt, es jedoch eine weitere Datenschutzregel gibt, welche den Zugriff auf alle Dokumente diesen Typs erlaubt.

Autorisierungsentscheidungen aufgrund von XACML PolicySets können in verschiedenen Ergebnissen enden:
Sollte ein PolicySet auf eine Anfrage anwendbar sein, so wird das Ergebnis der Datenschutzregel der Policy, welche auf die Anfrage angewandt wird, als Ergebnis des PolicySets zurückgegeben. Ein solches Ergebnis kann permit oder deny sein.
Zusätzlich können noch zwei weitere Ergebnisse zustande kommen, indeterminate, falls mehrere Datenschutzregeln auf die Anfrage anwendbar sind, oder not-applicable, falls keine Datenschutzregel anwendbar ist.

Es gibt zwei Arten von Entscheidungsverfahren, welche durch einen PEP implementiert werden können, permit-based oder deny-based.
Permit-based führt bei allen Entscheidungen, die nicht deny sind, zur Freigabe des Zugriffs. (permit-based PEP)
Deny-based führt bei allen Entscheidungen, die nicht permit sind, zur Ablehnung des Zugriffs. (deny-based PEP)

In dieser Arbeit wird von einem deny-based PEP ausgegangen.
Sollten also Anfragen an das PolicySet gestellt werden, die zu keinem eindeutigen Ergebnis führen, wird der Zugriff nicht gewährt.

Jeder Patient besitzt sein eigenes PolicySet. In diesem Set stehen die Datenschutzregeln, denen seine Dokumente unterliegen. Sollte eine Anfrage bezüglich eines Dokumentes eines Patienten in den PEP kommen, so muss sein PolicySet aus der DB abgefragt werden.
Die PolicySets müssen den ihnen zugehörigen Patienten eindeutig zugeordnet werden können.
Der PEP überprüft nun, ob das Resource-Element des PolicySets mit der Resource, welche in seiner Anfrage steht, übereinstimmt oder von ihr abgedeckt wird. Da in diesem An-

satz im Resource-Element des PolicySets der Ausdruck für die gesamte Akte des Patienten steht, ist diese Überprüfung immer wahr. Dies bedeutet, dass jede Anfrage auf Dokumente eines Patienten initial zur weiteren Überprüfung durch Auswertung des gesamten PolicySets akzeptiert wird. Der PEP sucht daher nun innerhalb des PolicySets nach einer Datenschutzregel, welche für dieses Dokument im Kontext der Anfrage anwendbar ist.

Das folgende Beispiel soll dies verdeutlichen:
Der PEP erhält eine Anfrage bezüglich des Zugriffs auf das Dokument
$file$:$ukhd$/$isis$/6723459/$medicalrecord$/$labresults$/$bloodtests$/$hivtest$30072010.pdf
des Patienten A mit der MPI-ID 6723459. Nun fragt der PEP das PolicySet des Patienten A aus der Datenbank ab und liest das Resource-Element des PolicySets aus. Dieses enthält $file$:$ukhd$/$isis$/6723459/$medicalrecord$/, die komplette Akte des Patienten.
Nun vergleicht der PEP die beiden Elemente mit der Vergleichsfunktion urn:oasis:names:tc:xacml:1.0:function:string-greater-than. Die Funktion prüft ob der String des Resource-Elementes des PolicySets im Anfrage-String enthalten ist. Da dies der Fall ist, liest der PEP nun den Rest des PolicySets aus, auf der Suche nach der Datenschutzregel, die sich auf die Anfrage bezüglich dieses Dokumentes anwenden lässt.

Dieses Ablaufverhalten kann man sich nun zu Nutze machen, indem man eine ”Major”-Policy innerhalb eines PolicySets definiert. Eine solche Policy beinhaltet Datenschutzregeln, die den Zugriff auf Organisations- und Patientenaktenebene regeln. Sie trifft Aussagen über den Zugriff einer Organisation auf alle Dokumente eines Patienten. Dies entspricht Anwendungsfall 1, siehe S,48.
Da der deny-based PEP grundsätzlich den Zugriff verweigert, falls keine Datenschutzregel auf die Anfrage anwendbar ist, müssen Regeln, welche auf Organisations- und Patientenaktenebene ein deny zur Folge hätten, nicht berücksichtigt werden. Sie können weggelassen werden.

Datenschutzregeln einer Major Policy haben daher grundsätzlich den Effekt Permit.
Die Major-Policy hat den Vorteil, dass Anfragen, welche aufgrund der Forderungen des Standards immer nur gezielt auf ein Dokument Zugriff verlangen und für die keine Datenschutzregel im PolicySet existiert, die das Dokument explizit erwähnt, auf die Datenschutzregeln der Major-Policy abgebildet werden können. Dies ist möglich, da die Datenschutzregeln der Major-Policy den Zugriff auf die gesamte Akte und alle darin beinhalteten Dokumente eines Patienten erlauben. Dies entspricht dem vorangegangenen Beispiel.

Zusätzlich zur Major-Policy, die den Zugriff auf alle Dokumente einer Patientenakte implizit erlaubt, gibt es noch weitere Policies die den Zugriff auf Dokumentenebene regeln. Zum einen die Dokumentengruppen-Policy, welche Datenschutzregeln beinhaltet, die den Zugriff

auf eine ganze Dokumentengruppe beschränkt, beispielsweise Bluttests, zum anderen die Dokumenten-Policy, in der Datenschutzregeln stehen, welche Aussagen über den Zugriff auf einzelne Dokumente treffen.

Die Abarbeitung der Policies erfolgt dabei entsprechend ihrer Reihenfolge innerhalb des PolicySets:

<PolicySet>
  <Policy> Dokumenten-Policy </Policy>
  <Policy> Dokumentengruppen-Policy </Policy>
  <Policy> Major-Policy </Policy>
</PolicySet>

Dies hat zur Folge, dass zuerst überprüft wird, ob eine Datenschutzregel innerhalb der Dokumenten-Policy auf die Anfrage anwendbar ist. Danach wird geprüft, ob das Dokument der Anfrage in einer Datenschutzregel der Dokumentengruppen-Policy beinhaltet ist. Falls auch dies erfolglos bleibt, wird geprüft, ob es eine grundlegende Datenschutzregel innerhalb der Major-Policy gibt, welche der anfragenden Organisation den Zugriff auf die gesamte Akte und damit auch auf das angefragte Dokument erlaubt. Sollte auch an diesem Punkt keine anwendbare Datenschutzregel gefunden werden, so wird der Zugriff aufgrund des deny-based PEP standardmäßig verweigert.

Das PolicySet gibt den Algorithmus first-applicable zur Verarbeitung der Policies innerhalb des PolicySets vor. Dies bedeutet, dass das Ergebnis der ersten gefundenen Policy, welche eine Datenschutzregel beinhaltet, die auf eine Anfrage anwendbar ist, als Ergebnis der Anfrage bezüglich Zugriff zurückgegeben wird. Eine weitere Betrachtung der Datenschutzregeln aller Policies findet nach einer gefundenen anwendbaren Datenschutzregel nicht mehr statt.
Durch die bottom-up Verarbeitung ist es möglich Spezialfälle abzubilden und den Zugriff auf einzelne Dokumente zu verwehren, den Zugriff auf die Gesamtheit der Dokumente allerdings effizient zu ermöglichen. Dieses Konzept würde wenige Datenschutzregeln innerhalb der Polices nach sich ziehen, wäre also in der Verarbeitung des PolicySets gegenüber einem PolicySet, in dem für alle Dokumente explizite Datenschutzregeln beschrieben würden, sehr schlank. In diesem Konzept würde man zuerst prüfen, ob die Anfrage auf die in den Policies beschriebenen, Spezialfälle passt und, sollte dies nicht der Fall sein, sich von dort auf die Major-Policy vorarbeiten. Bei einem PolicySet, in dem explizit für alle Dokumente eines Patienten Datenschutzregeln vorhanden sind, müsste man sehr viel mehr Datenschutzregeln verarbeiten, bis man einen Treffer landet. Dementsprechend wäre der Rechen- und Verwaltungsaufwand erheblich größer.

6 Implementierung

Die in Kapitel 3 beschriebene Technologiewahl und das im vorangegangenen Kapitel beschriebene Konzept der Einwilligungserklärungen hatten maßgeblichen Einfluss auf die Implementierung des Consent Creators. Dieses Kapitel soll die konkreten Ergebnisse der Implementierung aufzeigen und veranschaulichen, wie die Ergebnisse der Anforderungsanalyse (Siehe Kapitel 4) in Einklang mit dem entwickelten Konzept der Einwilligungserklärungen (siehe Kapitel 5) und der gewählten Technologie (siehe Kapitel 3) gebracht wurden.

6.1 Webservice

Wie bereits beschrieben wurde das Design der Oberfläche durch das Corporate Design des Universitätsklinikums Heidelberg bestimmt. Entsprechend finden sich die Bildwortmarken des Universitätsklinikums an prominenten Stellen der Oberfläche des Consent Creators wieder. Der hier beispielhaft angedeutete Begrüßungstext der Startseite, siehe Abbildung 15, sollte nach der Inbetriebnahme dazu genutzt werden, Patienten über ISIS aufzuklären und aktuelle Entwicklungen des CC bekannt zugeben. Der Menupunkt „Anmelden“ bietet den Benutzern die Möglichkeit sich im CC mit ihren bereits angelegten Profilen anzumelden. Die Anmeldung erfolgt dabei unter der Verwendung der während der Registrierung angegebenen Emailadresse und des Passwortes des Benutzers.
Benutzer die noch kein Profil besitzen können sich entsprechend unter dem Menupunkt „Registrieren“ im CC registrieren. Für die Registrierung im CC ist es erforderlich grundlegende Daten anzugeben, welche die eindeutige Identifikation des Benutzers erlauben. Zu den Daten gehören neben dem Namen des Benutzers auch seine Emailadresse, sein Geburtsdatum, sein Geschlecht und seine Anschrift. Wenn sich ein Benutzer registrieren möchte, wählt er im entsprechenden Menu die Funktion „Registrieren“ aus, der CC fragt mit den angegebenen Daten im MPI nach, ob bereits ein Benutzer mit diesen Daten dort existiert. Sollte dies nicht der Fall sein, so wird der Benutzer im MPI und im CC registriert. Die Identifikation des Benutzers, welche er im MPI besitzt wird dabei ebenso zur Identifikation im CC genutzt, entsprechend sind die beiden Profile verknüpft. Initial wird eine Null-Einwilligung (Siehe Glossar - Anhang A) für den Benutzer erstellt und an den Consent Manager gesendet. Es wird anschließend eine Email an den Benutzer gesendet, die es ihm ermöglicht ein Passwort zusetzen mit dem er sich im CC anmelden kann.
Im Falle eines bereits im MPI existierenden Profils, das mit den Daten des neuen Benutzers übereinstimmt, wird dieser nur im Datenbestand des CC registriert, sein Profil allerdings auch mit dem bereits im MPI bestehenden Profil verknüpft. Der Benutzer wird zum Schutz vor Identitätsdiebstahl jedoch nur als inaktiver Benutzer hinzugefügt. Es wird zusätzlich in der Datenbank des CC festgehalten, dass es bei der Registrierung dieses Benutzers zu

Abbildung 15: Webservice Oberfläche Startseite

einem Problem kam, welches die Aufmerksamkeit der Clearingstelle benötigt. Auch in diesem Fall wird eine Null-Einwilligung an den Consent Manager gesendet, der Patient erhält aufgrund der ungeklärten Situation keine Email um ein Passwort zu setzen.
Die Funktion „Passwort anfordern“ ermöglicht es einem Benutzer unter der Angabe seiner Emailadresse den CC aufzufordern, ihm eine Email zu senden, die es ihm ermöglicht, ein neues Passwort für sein Profil zu setzen. In dieser Email befindet sich ein Link dem der Benutzer folgt und über den es ihm möglich ist für sein Profil ein neues Passwort zu setzen. Es wird dabei über einen Referer sichergestellt, dass es nur dem Benutzer möglich ist, die Möglichkeit der Passwortänderung zu nutzen. Der Referer wird in Datenbank dem Benutzer zugeordnet, der mit dieser Emailadresse assoziiert ist. Der Referer wird durch Zufallsgeneration erzeugt und besitzt eine entsprechende Länge um Brute-force Angriffe sehr zeitintensiv werden zu lassen. Der Referer ist 72 Stunden aktivierbar, danach verfällt er und kann nicht mehr genutzt werden. Die selben Einschränkungen gelten für die Emails

zum Setzen eines Passwortes, welche im Falle einer Registrierung gesendet werden.
Der Menupunkt „Kontakt“ enthält neben den Informationen zur Kontaktierung des ISIS-Betreibers ebenso Informationen um mit der Clearingstelle in Kontakt zu treten. Durch diese Kontaktmöglichkeiten soll es interessierten Patienten möglich sein, Informationen, über die der Startseite hinaus, von den genannten Stellen zu erfragen.
Der Menupunkt „Impressum“ enthält die im Rahmen der Gesetzgebung geforderten Informationen zum Betreiber der Webseite.

Abbildung 16: Webservice Oberfläche Menu Patient

Angemeldete Benutzer erhalten je nach der Stufe ihrer Berechtigungen eine Darstellung der für sie verfügbaren Funktionalitäten. Im Falle des Patienten erhält dieser nur Zugriff auf Funktionen die ausschließlich Einstellungen seines Profils ändern (Abbildung 16). Der angemeldete Benutzer erhält in der Titelleiste des CC Informationen über seinen Status im CC und unter welchen Daten er angemeldet ist. Klickt er auf die Darstellung des Aus-

weises führt ihn dies zur Ansicht der Daten seines Profils. Die Funktionen „Abmelden“ in der Titelleiste und im Menu der Navigation besitzen die selbe Funktionalität und melden den Benutzer aus dem CC ab. Sollte diese Funktion genutzt werden führt sie den Benutzer zur Startseite des CC zurück, er muss sich erneut anmelden um den CC zu nutzen.
Die Funktion „Eigene Daten bearbeiten“ ermöglicht es dem Benutzer die Daten seines Profils zu aktualisieren. Auf Wunsch des ISIS-Betreibers ist es grundsätzlich möglich alle Daten eines Profils anzupassen. Sollte der Benutzer seine Daten speichern wollen, so wird vor Übernahme der Änderungen geprüft, ob bereits ein Benutzer im System registriert ist, der die entsprechenden Daten besitzt. Dies wird für die verwendete Emailadresse und die Vereinigung der Daten Name, Vorname, Geschlecht und Geburtsdatum geprüft. Es können zu keiner Zeit zwei Patienten die selben Werte für alle vier genannten Attribute aufweisen, da diese zur eindeutigen Identifikation genutzt werden. Emailadressen dürfen genauso nur einmal im CC vorhanden sein. Sollte die Suche nach einem Patienten in der Datenbank des CC mit den geänderten Daten erfolgreich sein, so wird geprüft ob der gefundene Patient mit dem editierenden Patienten übereinstimmt. Wenn dies der Fall ist, werden die Änderungen übernommen, andernfalls werden die Änderungen verworfen. Die Überprüfung findet anhand der ID des gefundenen Benutzers und des editierenden Benutzers statt. Ausgeschlossen von der direkten Änderung ist das Passwort des Benutzers, dieses kann nur über die Anfrage einer entsprechenden Email geändert werden.
Die Funktion „Einwilligungserklärung anzeigen“ stellt dem Benutzer seine aktuelle Einwilligungserklärung in menschenlesbarer Form im Format eines PDF zur Verfügung. Dieses PDF wird direkt aus dem Consent Manager abgefragt, wo es für diesen Fall vorgehalten wird. Der Benutzer kann sich so schnell einen Überblick verschaffen, welchen Datenschutzregeln seine in ISIS vorhandenen Dokumente momentan unterliegen und ob und welche Dokumente von wem in ISIS eingestellt werden dürfen.
Patienten die mit ihrer aktuellen Einwilligungserklärung unzufrieden sind und die Einwilligungserklärung in dieser Form nicht mehr für die Beschränkung des Zugriffs nutzen möchten, können diese durch Nutzung der Funktion „Einwilligungserklärung zurücksetzen“ auf eine standardisierte Einwilligungserklärung zurücksetzen. Im Falle von „Einwilligungserklärung zurücksetzen“ wird eine Einwilligungserklärung erstellt, die das Einstellen von neuen Dokumenten in ISIS zwar für alle an ISIS teilnehmenden Organisationen ermöglicht, es jedoch keiner Organisation ermöglicht die Dokumente des Patienten einzusehen. Von dieser Einwilligungserklärung ausgehend kann der Patient dann seine neuen Vorgaben in einer Einwilligungserklärung umsetzen.
Eine weitere Möglichkeit eine standardisierte Einwilligungserklärung zu erzeugen ist die Auswahl der Funktion „Teilnahme beenden“. Diese Funktion erzeugt eine Null-Einwilligungserklärung (Siehe Glossar - Anhang A). Zusätzlich wird der Benutzer nach Abschluss dieses Use Cases inaktiviert und abgemeldet. Um die Einwilligungserklärungen der beiden vorherigen Funktionen rechtskräftig zu signieren ist es dem Patienten möglich,

zwischen zweierlei Verfahren auszuwählen (Abbildung 17).

Abbildung 17: Webservice Oberfläche Wahl der Signatur

Eines der Verfahren ist die digitale Signatur. Vorraussetzung hierfür ist der Besitz einer sicheren Signaturerstellungseinheit (SSEE) und eines entsprechenden Zertifikates, gespeichert auf einem mit der SSEE verwendbaren Medium. Ist der Patient im Besitz dieser Objekte kann er die Einwilligungserklärung mit einer qualifizierten elektronischen Signatur versehen. Hierfür stellt der CC ein Java Applet zur Verfügung. Das Applet fordert den Benutzer auf den Treiber seiner SSEE auszuwählen und seinen, für die Erzeugung der Signatur benötigten, PIN einzugeben. Das Applet versucht anschließend die standardisierte Einwilligungserklärung, welche zum Start des Applets vom CC im CDA Format abgefragt wurde, mit einer Signatur zu versehen. Sollte dies gelingen wird die Einwilligungserklärung an den CC übermittelt, welcher diese an den Consent Manager weiterleitet. Im Falle der Funktion „Teilnahme beenden“ wird, wie bereits erwähnt, der Benutzer abschließend de-

aktiviert und abgemeldet.
Sollte der Benutzer nicht über eine SSEE verfügen, kann er die Einwilligungserklärung dennoch auch von zuhause erfolgreich signieren. Hierfür wurde das Konzept der Speicherung einer unsignierten Einwilligungserklärung etabliert. Basis dieses Konzeptes ist es, dem Benutzer die Einwilligungserklärung zur Unterschrift zur Verfügung zu stellen und ihm die Möglichkeit zu geben, diese Einwilligungserklärung unterschrieben per Post an die Clearingstelle des intersektoralen Informationssystems zu senden. Sollte der Benutzer die Funktion „Schriftliche Signatur“ wählen wird ihm ein Menu angezeigt, welches ihm die weiteren Schritte erklärt. Diese sind zu einen das Bestätigen der Signierung nach diesem Schema. Bestätigt der Benutzer wird die Einwilligungserklärung entsprechend des Kontextes der Funktion erstellt, welche zur Wahl der Signaturmethode geführt hat. Diese Einwilligungserklärung wird dem Patienten in Form eines PDFs zur Verfügung gestellt. Dieses PDF druckt er aus und sendet die handschriftlich unterschriebene Einwilligungserklärung an die Clearingstelle. Der CC erstellt nach der Bestätigung durch den Patienten die Einwilligungserklärung im CDA Format. Er erzeugt einen MD5 Hash des Dokumentes. Er dokumentiert die Wahl der schriftlichen Signatur in der Datenbank und erstellt einen zufälligen Schlüssel der als Dateiname der Einwilligungserklärung für die Speicherung der Einwilligungserklärung im Dateisystem des CC genutzt wird. Diesen vermerkt er ebenso in der Datenbank. Dann sendet er den MD5 Hash des Dokumentes an den Consent Manager. Sobald die Einwilligungserklärung in der Clearingstelle eingetroffen ist und einer Überprüfung durch das Personal standgehalten hat, wird sie freigeschaltet. Dies bedeutet die Übermittlung der im Dateisystem des CC gespeicherten Einwilligungserklärung an den Consent Manager. Dieser prüft die Authentizität der Einwilligungserklärung durch den gespeicherten MD5 Hash und setzt dann die Datenschutzregeln der jeweiligen Einwilligungserklärung durch.
Im Falle der Beendigung der Teilnahme durch den Patienten und der Wahl des Verfahrens der schriftlichen Signatur wird das Profil des Benutzers erst nach Eintreffen der Einwilligungserklärung in der Clearingstelle und deren Freischaltung deaktiviert. Dies liegt darin begründet, dass bis zum Zeitpunkt der Freischaltung keine rechtlich verbindliche Einwilligungserklärung vorliegt, welche den Willen des Patienten zur Beendigung der Teilnahme bekundet.
Die Wahl zwischen den beiden Verfahren macht es auch für technisch nicht versierte Benutzer möglich, den Consent Creator erfolgreich und für sie zufriedenstellend zu nutzen ohne dabei in einer an ISIS teilnehmenden Organisation vorstellig werden zu müssen.
Zusätzlich zur Wahl der Form der Einwilligungserklärung kann der Patient sich im gezeigten Menu Informationen über das jeweilige Verfahren anzeigen lassen.

Die beiden bisher beschriebenen Funktionen zur Erstellung einer Einwilligungserklärung lassen dem Benutzer keine Freiheiten in der Wahl der in der Einwilligungserklärung enthaltenen Datenschutzregeln. Da es das Ziel des Consent Creator ist, personalisierte Ein-

Abbildung 18: Webservice Oberfläche Einwilligungserklärung erstellen

willigungserklärungen zu erstellen, bietet der CC die Funktion „Einwilligungserklärung erstellen“ an (Abbildung 18). Mit Hilfe dieser Funktion ist es dem Patienten möglich, eigene Datenschutzregeln nach seinen persönlichen Vorgaben zu erstellen, welche dann in einer durch XACML auswertbaren Form im CDA Format der Einwilligungserklärung festgehalten werden. Für die Darstellung des Menus wird ein Java Applet genutzt das durch den ISIS-Betreiber signiert wurde um dem Applet erweiterte Funktionalität zu ermöglichen. Zu diesen Funktionalitäten gehören der Aufbau von Verbindungen zum Consent Creator und die Auswahl von lokalen Dateien. Ersteres wird für den Datenaustausch mit dem CC benötigt, letzteres für die digitale Signatur der Einwilligungserklärung, sollte diese Form der Signatur gewählt werden.

Sobald das Applet geladen wurde fragt dieses die benötigten Informationen zur Darstellung aus dem CC ab. Die Darstellung enthält dabei auch die Datenschutzregeln der bisherigen Einwilligungserklärung, welche in einer Liste dargestellt werden. Der Benutzer kann Datenschutzregeln aus der Einwilligungserklärung löschen indem er die Datenschutzregel durch einen Rechtsklick auswählt und im sich öffnenden Kontextmenu die Funktion „Löschen“ auswählt.
Eine neue Datenschutzregel kann der Patient durch die Zusammenstellungsmöglichkeiten in der Mitte des Applets erstellen. Die einzelnen Elemente ermöglichen durch die Kombination ihrer Inhalte die differenzierte Zusammenstellung einer Datenschutzregel gemäß der Vorgaben des Patienten. Der Baum der Organisationen zeigt dem Patienten die an ISIS teilnehmenden Organisationen an. Er kann dann durch Seleketion einer Organisation eine Datenschutzregel erstellen, welche diese Organisation betrifft. Durch automatische Selektion der Unterorganisation der durch den Patienten gewählten Organisation wird dem Patienten verdeutlicht, dass diese Organisationen durch die momentan gewählte Datenschutzregel ebenfalls betroffen sind. Die Darstellung der an ISIS teilnehmenden Organisationen wird dabei stufenweise aus dem CC abgefragt, so die Äste des Baums durch den Patienten erweitert werden. Dies liegt in der Anzahl der Organisationen begründet, den kompletten Baum bei jedem Aufruf des Applets zu senden würde bedeuten enorme Datenmengen an die aufrufenden Clients verteilen zu müssen. Es ist dem Patienten nur möglich zu jedem Zeitpunkt eine Organisation und deren Unterorganisationen auszuwählen. Dies liegt darin begründet, den Patienten anzuhalten nur Datenschutzregeln zu erstellen, deren Wirkung er auf einen Blick abgeschätzen kann. Zudem wäre die Sortierung der Datenschutzregeln innerhalb des PolicySets bei mehreren betroffenen Organisationen auf unterschiedlichen Ebenen der Organisationshierarchie nicht mehr möglich.
Die Auswahlmöglichkeiten beschränken sich nicht nur auf die Organisation selbst, sondern es können auch aus dem Personal der Organisation Untergruppen gewählt werden. Während „Alle“ den Zugriff für alle Personengruppen der Organisation beschränken würde, könnte der Patient etwa durch Auswahl von „Ärzte“ im entsprechenden Feld den Zugriff nur für die Ärzteschaft der Organisation beschränken.
Der Zugriff lässt sich im gleichen Maß auch für die Dokumente des Patienten differenziert beschränken. Wie für die Wahl der Personen gibt es auch für die Wahl der Dokumente den Wert „Alle“. Darüber hinaus kann der Patient aus einer Liste bestehend aus allen in ISIS vorhandenen Dokumententypen auswählen. Durch diese Auswahlmöglichkeit kann der Patient beispielsweise den Zugriff auf seine Laborberichte beschränken.
Des Weiteren ist es dem Patient möglich die Art des Zugriffes festzulegen, welcher der Datenschutzregel zugrunde liegt. Dies können Schreib- oder Lesevorgänge sein. Es ist auch möglich die Kombination der Vorgänge als Zugriffsart festzulegen, beispielsweise um sowohl das Einstellen als auch das Lesen von Dokumenten in ISIS zu beschränken. Letztlich obliegt es dem Patienten, ob er Zugriff gewähren oder verwehren möchte. Die Auswahl

kann durch „Zugriff zulassen“ getroffen werden. Es kann nur zwischen den Werten „Ja“ und „Nein“ gewählt werden.
Sollte der Patient mit der Formulierung seiner Datenschutzregel zufrieden sein, kann er diese durch die Funktion „Datenschutzregel hinzufügen“ zu seinem PolicySet hinzufügen. Die Datenschutzregel wird durch diesen Vorgang lediglich im PolicySet des Patienten vermerkt, dieser Vorgang entspricht nicht einer endgültigen Speicherung der Datenschutzregel. Durch die Funktion „Verwerfen“ werden die Felder der Auswahlmöglichkeiten auf die Standardwerte zurückgesetzt.
Die Formulierung der durch den Patienten zusammengestellten Datenschutzregel wird dabei stets in der Darstellung „Aktuelle Datenschutzregel“ angezeigt. Diese Darstellung vollzieht jede Änderung der Werte in den Auswahlmöglichkeiten sofort nach um dem Patienten eine sofortige Rückmeldung über die Tragweite seiner Entscheidungen zu vermitteln. Durch die sofortige Änderung der Darstellung soll zudem ein Lerneffekt erreicht werden, der die künftige Nutzung des CC für den Patienten einfacher gestalten soll.
Sollte der Patient versuchen eine Datenschutzregel zu formulieren deren Effekt in dieser Form nicht auftreten kann wird er darüber informiert, dass diese Datenschutzregel nicht unterstützt wird. Ein Beispiel für eine solche Datenschutzregel wäre „Alle Ärzte der Organisation Universtitätsklinikum Heidelberg dürfen weder meine Arztbriefe in ISIS einstellen noch in ISIS eingestellte Dokumente diesen Types lesen“. Diese Datenschutzregel wird vor dem Hintergrund, dass nur Organisationen Dokumente in ISIS einstellen, nicht unterstützt. Entsprechende Erklärungen welche dem Patienten die Grenzen der Erstellung aufzeigen sind in der Hilfe des Erstellungsmenus zu finden.
Sobald der Patient mit der Zusammenstellung der Datenschutzregeln seiner Einwilligungserklärung zufrieden ist, wählt er die Funktion „Einwilligungserklärung speichern“ aus. Es öffnet sich im Applet die Möglichkeit zur Wahl der Signatur. Auch hier bietet sich dem Patienten wie in den bereits beschriebenen Fällen, die eine Signatur erforderten, die Wahl zwischen einer digitalen Signatur der Einwilligungserklärung oder der Speicherung der unsignierten Einwilligungserklärung, bis zu ihrem Eintreffen in der Clearingstelle. Durch die Kombination des Erstellungsapplets mit dem Signaturapplet ist es ohne erneutes Laden eines weiteren Applets möglich die Einwilligungserklärung digital zu signieren.
Die Summe der Funktionen des Menus für Patienten geben dem Patienten alle Möglichkeiten an die Hand, eine Einwilligungserklärung nach seinen Vorgaben zu erstellen und seine Teilnahme an ISIS so zu gestalten wie er dies möchte.

Einem Benutzer in der Rolle eines Leistungserbringers bieten sich aufgrund seiner Aufgaben verschiedene Funktionalitäten an (Abbildung 19).
Es ist einem Leistungserbringer grundsätzlich möglich Benutzer über die Funktion „Teilnehmer hinzufügen“ hinzuzufügen. Wie im bereits beschriebenen Falle der Registrierung eines Teilnehmers muss auch der Leistungserbringer die entsprechenden Daten angeben,

Abbildung 19: Webservice Oberfläche Menu Leistungserbringer

die für eine Registrierung erforderlich sind. Anders als im Falle der Registrierung eines Benutzers aus eigenem Bestreben, in dem eine Null-Einwilligung erzeugt wird, muss der Leistungserbringer für den Benutzer nach dem Vorgang des Hinzufügens eine Einwilligungserklärung erstellen. Diesem Ablauf zugrunde liegt die gewünschte Teilnahme des zu registrierenden Benutzers, welche jedoch nicht durch eine mündliche Absprache ausreichend und rechtlich verbindlich dokumentiert wird. Für den Leistungserbringer besteht, wie für einen Patienten auch, die Möglichkeit zwischen den beiden Signaturverfahren zu wählen. Der Ablauf der Signaturverfahren entspricht den bereits beschriebenen Verfahren für Patienten, einzig obliegt es bei der Speicherung einer unsignierten Einwilligungserklärung dem Leistungserbringer, die Unterschrift des Patienten einzuholen und die Einwilligungserklärung an die Clearingstelle zu übersenden. Die Signatur der Einwilligungserklärung mittels des Verfahrens der digitalen Signatur geschieht mit dem privaten Schlüssel des Leistungserbringers.

Zusätzlich ist es dem Leistungserbringer nach der neuerlichen Registrierung eines Teilnehmers möglich, eine personalisierte Einwilligungserklärung über das Einwilligungserstellungs-Applet für den Teilnehmer zu erstellen. Diese Funktionalität ist nötig um Patienten, welche gerade in der Organisation des Leistungserbringers vorstellig und an ISIS teilnehmen möchten, zeitnah in das Projekt einzubinden und ihnen eine Einwilligungserklärung zu erstellen, mit der es dem Leistungserbringer möglich ist, die neuerlich anfallenden Dokumente direkt in ISIS einzustellen und diese an der Behandlung beteiligten Organisationen zur Verfügung zu stellen, so dies der Patient wünscht.
Zu den Möglichkeiten des Leistungserbringers gehört es auch, über die Funktion „Einwilligungshistorie ansehen“ nach einem Patienten zu suchen und eine Liste aller bisher erstellten Einwilligungen des Patienten zu erhalten. Aus dieser Liste, welche aus Informationen zu den Erstellungszeitpunkten der Einwilligungserklärungen besteht, kann der Leistungserbringer eine einzelne Einwilligungserklärung auswählen. Diese Einwilligungserklärung wird dann als PDF vom Consent Manager erfragt und dem Leistungserbringer zur Verfügung gestellt.
Die Funktion „Teilnehmer bearbeiten“ ermöglicht es dem Leistungserbringer nach einem Teilnehmer zu suchen und sich dessen Daten anzeigen zu lassen. Kriterien für die Suche sind Name, Vorname, Geschlecht und Geburtsdatum. Anhand dieser Kriterien wird der Benutzer in der Datenbank des CC gesucht, sollte er gefunden werden so werden seine Daten für die Bearbeitung angezeigt. Dem Leistungserbringer ist es möglich alle Daten eines Teilnehmers zu bearbeiten, das Passwort ist hiervon ausgeschlossen, es wird nicht angezeigt. Für die Speicherung der Änderungen gelten die selben Beschränkungen wie im Falle eines Patienten der seine Daten bearbeitet hat und speichern will; es ist nicht möglich Daten so zu ändern, dass Name, Vorname, Geschlecht und Geburtsdatum oder die Emailadresse zweier Teilnehmer übereinstimmen.
Die Funktionen „Teilnehmer aktiveren“ aktiviert einen zuvor deaktivierten Teilnehmer in der Datenbank. Vor der Aktivierung wird der Leistungserbringer aufgefordert den Teilnehmer anhand dessen Stammdaten zu identifizieren. Sollte ein Benutzer mit übereinstimmenden Daten gefunden werden, wird dieser Benutzer dem Leistungserbringer mit all seinen persönlichen Daten zur Bestätigung angezeigt. Bestätigt der Leistungserbringer die Aktivierung wird der Teilnehmer in der Datenbank des CC aktiviert. Anschließend wird eine Email an den Teilnehmer gesendet, die es ihm ermöglicht ein neues Passwort für sein wieder aktives Profil zu setzen. Der Leistungserbringer wird nach der erfolgreichen Aktivierung aufgefordert, eine Einwilligungserklärung zu erstellen, welche die erneute Teilnahme des Teilnehmers an ISIS dokumentiert. Es wird in diesem Fall eine standardisierte Einwilligungserklärung erstellt, welche das Einstellen von Dokumenten des Teilnehmers in ISIS erlaubt, jedoch den Zugriff auf die Dokumente des Teilnehmers verbietet.
Für die Signatur der Einwilligungserklärung stehen dem Leistungserbringer die beiden bereits beschriebenen Verfahren zur Verfügung.

Die Funktion „Teilnehmer inaktivieren“ hat den selben Ablauf wie „Teilnehmer aktivieren“, einzig der Effekt der Funktion ist gegenteilig, es wird zudem keine Email an den Benutzer gesendet und die zu erstellende Einwilligungserklärung verbietet sowohl das Einstellen neuer Dokumente des Patienten als auch das Abfragen bereits eingestellter Dokumente.

Abbildung 20: Webservice Oberfläche Menu Administrator

Administratoren besitzen das besondere Vertrauen des ISIS-Betreibers, zu dieser Personengruppe gehört beispielsweise das Personal der Clearingstelle. Da Administratoren in der Hierarchie der Benutzergruppen über der Personengruppe der Leistungserbringer rangieren haben sie Zugriff auf alle Funktionen, die Leistungserbringern zur Verfügung stehen. Zusätzlich besitzen Administratoren allerdings noch Zugriff auf zwei wesentliche Funktionen die zur Administration des Consent Creators und damit zum reibungslosen Betrieb desselben nötig sind (Abbildung 20).
Da sich Benutzer, welche bereits im MPI eingetragen, allerdings noch nicht im CC regis-

triert sind, neuerlich im CC registrieren können, muss geprüft werden, ob das Registrierungsbestreben der jeweiligen Benutzer auch vom Benutzer ausgeht und nicht von Dritten. Registrierungsversuche welche von den Benutzern mit dem beschrieben Hintergrund ausgehen werden deshalb zwar nicht abgelehnt, jedoch wird der Benutzer wie bereits beschrieben als inaktiv hinzugefügt und seine Registrierung bedarf der Freischaltung durch die Clearingstelle. Hierfür ist ein Administrator in der Lage die Funktion „Benutzer freischalten“ zu nutzen. Nach der Auswahl dieser Funktion werden dem Benutzer alle Teilnehmer angezeigt, bei deren Registrierung bereits ein Eintrag im MPI vorhanden war. Der Administrator kann nun auswählen ob er den Benutzer freischalten oder die Registrierung ablehnen möchte.
Sollte er sich dazu entschließen den Benutzer freizuschalten, wird dieser in der Datenbank aktiviert und es wird ihm eine Email zum Setzen eines Passwortes gesendet. Nach dem Setzen eines neuen Passwortes ist es dem Benutzer möglich sich anzumelden und den CC nach seinen Wünschen zu nutzen. Der Administrator wird nach dem Freischalten des Benutzers aufgefordert den Vorgang durch Erstellung einer Einwilligungserklärung für den Patienten entsprechend zu dokumentieren. Die Einwilligungserklärung ist standardisiert und erlaubt lediglich das Einstellen neuer Dokumente des Patienten in ISIS. Der Zugriff wird für alle Dokumente des Patienten verwehrt.
Entscheidet sich der Administrator den Benutzer nicht freizuschalten, so wird der Benutzer aus der Datenbank gelöscht. In diesem Fall wird keine Einwilligungserklärung erstellt.
Da es allen Benutzergruppen möglich ist, Einwilligungserklärungen unsigniert zu speichern und im CC vorhalten zu lassen, bis diese freigeschaltet werden, bietet der CC Administratoren über die Funktion „Einwilligungserklärung freischalten“ die entsprechenden Funktionen zum Abschließen dieser Vorgänge. Nach Auswahl der Funktion werden dem Administrator alle Benutzer angezeigt, die sich für eine Einwilligungserklärung mit schriftlicher Signatur entschieden haben. Der Administrator kann dann anhand der vorliegenden Einwilligungserklärung den Benutzer in der Liste suchen und die Einwilligungserklärung freischalten oder ablehnen.
Sollte sich der Administrator entschließen die Einwilligungserklärung des gesuchten Benutzers freischalten zu wollen gleicht er vorher noch das Datum mit dem Erstellungszeitpunkt der Einwilligungserklärung der Papierform mit dem Eintrag ab, welcher sich in der Darstellung im CC befindet. Stimmen die Daten überein kann die Einwilligungserklärung freigeschaltet werden. Der CC sucht nun die Einwilligungserklärung in seinem Dateisystem und sendet sie zusammen mit der ID des Benutzers, zu dem die Einwilligungserklärung gehört, an den Consent Manager. Dieser prüft die Authentizität des Dokumentes durch Erstellung eines MD5 Hashes und Abgleich dieses Hashes mit dem gespeicherten Hash, welchen der Cosent Manager zum Zeitpunkt der Wahl der schriftlichen Signatur durch den Benutzer vom CC erhalten hat. Sollten die Hashes übereinstimmen akzeptiert der Consent Manager die Einwilligungserklärung und setzt die enthaltenen Datenschutzregeln um.
Entscheidet sich der Administrator die Einwilligungserklärung abzulehnen, löscht der CC

die Einwilligungserklärung aus seinem Dateisystem und entfernt den entsprechenden Eintrag aus seiner Datenbank. Abschließend teilt er dem Consent Manager die Ablehnung mit, dieser verwirft den gespeicherten MD5 Hash. Die bisherige Einwilligungserklärung behält ihre Gültigkeit.

Die Implementierung des Baumes der Darstellung der an ISIS teilnehmenden Organisationen wurde von Santosh Kumar T.[22] übernommen und für die Zwecke des Consent Creators angepasst. Die Implementierung des Baumes ist unter der LPGL v2.1 Lizenz verfügbar.

Um die Einwilligungserklärungen mit einer digitalen Signatur zu versehen wurde auf die bereits bestehende Implementierung[23] von Nikolay Nedyalkov und Svetlin Nakov zurückgegriffen und diese für die Signierung eines XML Dokumentes angepasst.

6.2 Server

Die Implementierung des Servers bietet die Funktionalitäten um die Darstellung der beschriebenen Oberfläche zu ermöglichen. Die Implementierung entspricht dem standardgemäßen Aufbau eines Webservices einer Model2-Architektur. Das Klassendiagramm der Implementierung dieser Architektur befindet sich in Anhang B.2. Die Anfragen werden von Servlets verarbeitet und Antworten auf Anfragen werden über JSPs zurückgegeben. Die in der Anforderungsanalyse festgestellten benötigten Funktionen wurden aufgrund der Forderung der Wartbarkeit auf Servlets verteilt. Einzelne Servlets beinhalten dabei alle benötigten Aufrufe, beziehungsweise Antworten, welche für die Abarbeitung eines Use Case benötigt werden. Die Abläufe der Anfrageverarbeitung werden in den entsprechenden Sequenzdiagrammen der Use Cases dargestellt, diese befinden sich in Anhang B.3. Die einzelnen Servlets sind wiederum durch vorangestellte Filter geschützt. Die Filter dienen dazu, illegale Aufrufe zu verhindern und nur Aufrufe weiterzuleiten die der festgelegten Anfragesyntax folgen. Um die Servlets nur den für sie bestimmten Benutzergruppen zugänglich zu machen gibt es einen Filter der prüft, ob der Benutzer angemeldet ist. Sollte er dies nicht der Fall sein, erhält der Benutzer eine entsprechende Nachricht mit der Forderung sich vor der Nutzung des Consent Creators anzumelden, der Aufruf wird nicht weiter verarbeitet. Zusätzlich gibt es noch zwei weitere Filter, einer der beiden prüft ob der Benutzer ein Patient ist, mit dem Ziel Anfragen an Servlets welche nur Funktionen für Patienten bieten nur Patienten zur Verfügung zu stellen. Ebenso gibt es auch einen Filter der die Funktionen der privilegierten Benutzer schützt. Dies ist besonders wichtig da es ansonsten allen Benutzern möglich wäre, für privilegierte Benutzer reservierte Funktionen aufzurufen.

[22] *http://www.jroller.com/santhosh/entry/jtree_with_checkboxes*

[23] *http://www.developer.com/java/other/article.php/3587361/Java-Applet-for-Signing-with-a-Smart-Card.htm*

Durch diese Unterscheidung war es nötig, teilweise zwei Servlets für die Ausführung des nahezu identischen Progammablaufs zu implementieren. Dies ist beispielsweise für die Use Cases „Registrierung“ und „Teilnehmer hinzufügen“ der Fall. Durch die Sicherheitsmaßnahme der Trennung der Funktionen und der Verteilung des beinah selben Codes auf zwei Klassen wurde zwar die Wartbarkeit erschwert, der Sicherheitsaspekt wiegt in der sensiblen Anwendungsumgebung des Consent Creator jedoch schwerer.
Die Servlets beinhalten nur wenig Logik, sie greifen auf den darunterliegenden ConsentCreatorService zu, welcher ihnen die für die Verarbeitung der Anfrage benötigten Funktionen bietet. Der ConsentCreatorService wurde nach dem Singleton-Pattern implementiert, da er den Baum der Organisationen im Speicher halten muss. Aufgrund der Anzahl der Servlets und der erwarteten Größe des Baumes im zweistelleigen Megabytebereich würde es ansonsten zu einem massiven Arbeitsspeicherverbrauch kommen, würde jedes Servlet einen eigenen ConsentCreatorService instanzieren.
Der ConsentCreatorService selbst greift auf die Worker-Klassen DocumentFactory, Database und Shipper zu. Die DocumentFactory beinhaltet alle Datei- und XML-Operationen, die Database stellt Methoden für den Datenbankzugriff zur Verfügung und der Shipper ermöglicht es dem Consent Creator Daten an Teilsysteme der Anwendungsumgebung und Patienten per Email zu senden.
Die Trennung der Funktionalitäten nach Thematik soll die Wartbar- und Erweiterbarkeit des Consent Creators sicherstellen.
Auf die Implementierung der Klasse Shipper wurde verzichtet, da sich die anderen Teilsysteme zum Zeitpunkt dieser Arbeit teilweise noch im Aufbau befanden.
Das Rechtemanagement wurde in einer Basisversion implementiert, es gibt drei Anwenderklassen, welche jedoch keine expliziten Rechte besitzen. Für das erarbeitete Anwendungsszenario bietet diese Rechteverwaltung jedoch alle benötigten Informationen zur Verwaltung und Verfügungstellung der Funktionen des CC.
Die Informationen für die Konfigurationen der Komponenten und die für die Generation des CDA Dokumentes benötigten Informationen wurden in XML Dokumenten festgehalten. Dies macht es auch ohne das Neustarten des Servers möglich die Konfigurationen auszutauschen. Die Verbindung zur Datenbank lässt sich durch Proxool einfach per Konfigurationsdatei ändern, hierfür ist es nicht nötig den Code der Klasse Database anzupassen.

6.3 Datenbank

Das Datenbankschema (Abbildung 21) des Consent Creators bildet die Daten der Benutzer in einer zentralen Tabelle ab. Die Tabelle „users“ enthält die für die Speicherung benötigten Datenfelder mit dem primären Schlüssel „id“. Der Wert dieses Feldes entspricht für Patienten der MPI-ID. Im Falle von Profilen von Leistungserbringern, welche bei der Registrierung keine MPI-ID erhalten, da sie kein Patient sind und keine Daten in ISIS

einstellen, erhalten diese eine generierte ID, welche länger ist als eine MPI-ID. Dies ist nötig um die Eindeutigkeit der ID sicherzustellen. Die Daten jedes Benutzers unterliegen einer zusätzlichen Bedingung, es ist nicht möglich zwei Benutzer mit den selben Werten für die Vereinigung der Felder „name“, „forename“, „gender“ und „birthdate“ in die Tabelle einzufügen. Dies liegt darin begründet, dass diese Daten für die Suche nach Benutzern genutzt werden und daher eindeutig sein müssen. Der Consent Creator unterstützt zu diesem Zeitpunkt keine Suchanfragen welche zu mehreren Benutzern passen könnten.
Die Tabelle „unclearedconsents“ enthält die Einträge welche im Use Case „Einwilligungserklärung unsigniert speichern“ erzeugt werden. Enthalten sind neben der referenzierten ID des Benutzers auch der Dateiname der zum Benutzer gehörenden Einwilligungserklärung und deren MD5 Hash. Um die verzögerte Abarbeitung von De- und Aktivierungen zu ermöglichen wird die Information über den Teilnahmestatus ebenfalls in der Tabelle vermerkt. Um die eingetroffene Einwilligungserklärung zeitlich zuordnen zu können wird der Erstellungszeitpunkt der Einwilligungserklärung ebenfalls vermerkt. In der Tablle „registerconflicts“ werden die Vermerke über Benutzer gespeichert, welche bereits im MPI aber noch nicht im Consent Creator registriert sind. Entsprechend wird der auftretende Konflikt während der Registrierung in der Datenbank festgehalten. Zu den Informationen gehört lediglich ein Zeitstempel und die referenzierte ID des Benutzers. Über den Zeitstempel ist es möglich den Registrierungsversuch in Absprache mit dem Benutzer zu klären und diesen dann freizuschalten oder zu löschen.
Anfragen nach neuen Passwörtern werden in der Tabelle „passwordrequests“ gespeichert. Neben der referenzierten ID des Benutzers werden auch seine Emailadresse und der Zeitpunkt der Anfrage gespeichert. Der Zeitpunkt ist nötig um den ebenfalls gespeicherten Referer nach einer vorgegebenen Zeitspanne ablaufen zu lassen. Die RefererID wird genutzt die Echtheit der Anfrage des Benutzers zu bestätigen, es ist nur möglich mit einer Referer-ID ein neues Passwort zu setzen.
Das Datenbankschema bietet mit der zentralen Tabelle welche die Stammdaten eines jeden Benutzers enthält die Möglichkeit weitere Informationen einfach in weiteren Tabellen zur Verfügung zu stellen, Referenzierung der ID eines jeden Benutzers in den neuen Tabellen vorausgesetzt.

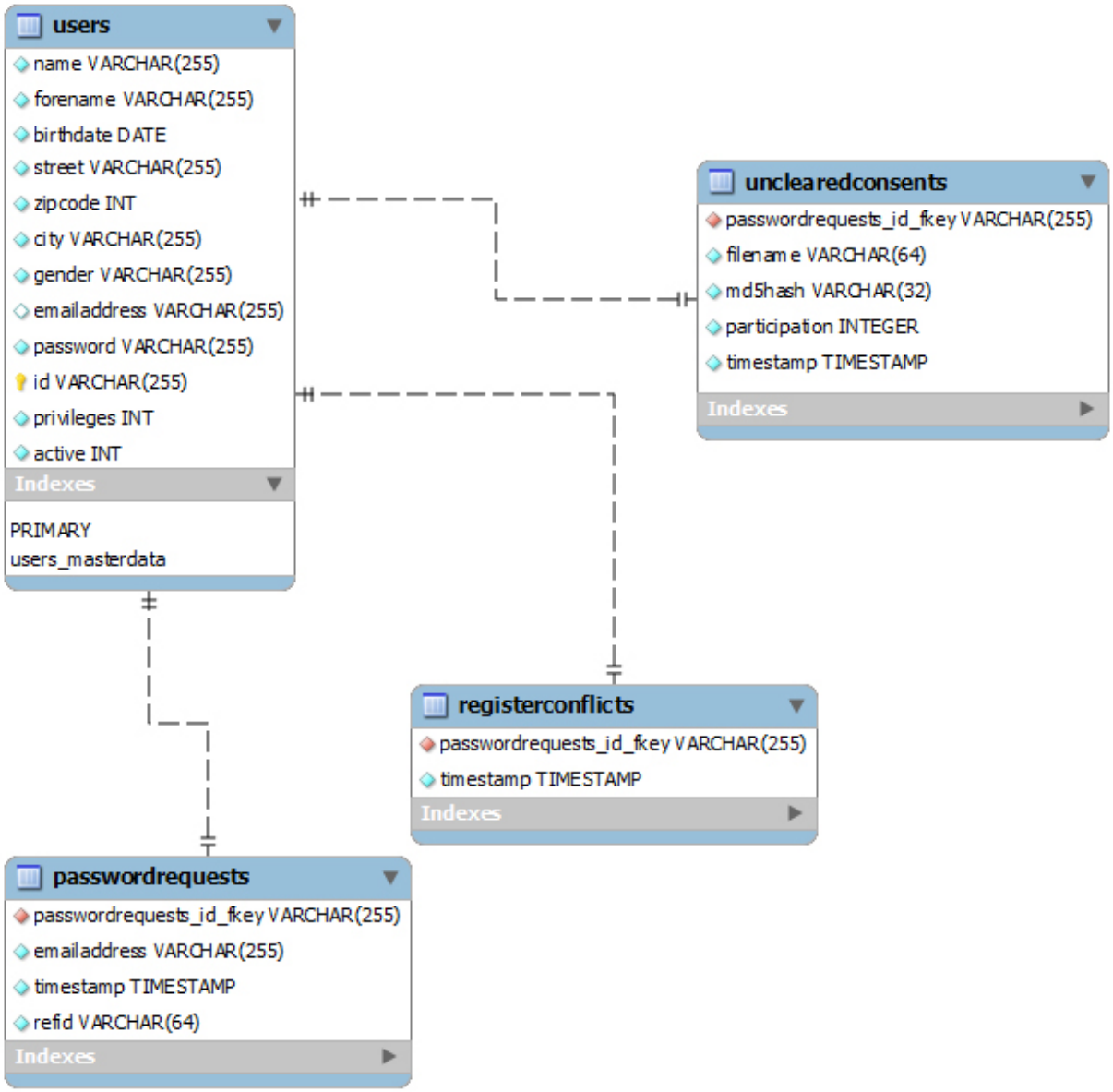

Abbildung 21: Datenbank-Schema

7 Test

7.1 Formale Prüfung

Die Implementierung des Consent Creators und seiner Methoden wurde mit JUnit-Tests getestet. Die Test Methoden beschränken sich dabei auf Vorgänge, bei denen eine maschinelle Überprüfung durchführbar ist. Ausgeschlossen ist davon beispielsweise die Überprüfung des Ergebnisses der Sortierung der Rule-Elemente einer Policy.

Test: Datenbanktests
Getestete Methoden: Alle öffentlichen Methoden der Klasse Database
Testbeschreibung: Zunächst wird ein neues User Objekt erzeugt. Dieses Objekt wird dann in der Datenbank gespeichert, anschließend wird geprüft ob unter den Daten des Benutzers ein Benutzer in der Datenbank vorhanden ist. Dieser Benutzer wird dann über die verschiedenen Methoden der Datenbank abgefragt. Anschließend wird der Benutzer deaktiviert, aktiviert und ein Password wird für ihn angefordert. Es wird geprüft ob in der Datenbank eine entsprechende Anfrage gespeichert wurde. Der Benutzer wird über die ID der Passwortanfrage aus der Datenbank abgefragt. Die ID der Passwortanfrage wird gelöscht. Das Passwort des Benutzers wird aus der Datenbank abgefragt. Der Benutzer wird geupdatet. Das Passwort des Benutzers wird geupdatet. Es wird geprüft ob das Passwort des Benutzers mit dem aus der Datenbank abgefragten Passwort des Benutzers übereinstimmt. Es wird ein Registrierungskonflikt für den Benutzer gespeichert. Der Konflikt wird über die Liste der Konflikte aus der Datenbank abgefragt. Der Konflikt wird gelöscht. Eine unsignierte Einwilligungserklärung wird für den Benutzer in der Datenbank festgehalten. Es wird geprüft ob eine unsignierte Einwilligungserklärung für den Benutzer in der Datenbank festgehalten wurde. Der Dateiname der unsignierten Einwilligungserklärung wird aus der Datenbank abgefragt. Die Liste der Benutzer mit unsignierten Einwilligungserklärungen wird abgefragt. Der Eintrag über eine unsignierte Einwilligungserklärung für den Benutzer wird gelöscht. Der Benutzer wird aus der Datenbank gelöscht. Es wird geprüft ob der Benutzer in der Datenbank existiert.
Erfolgsbedingungen: Alle Methoden liefern die erwarteten Rückgaben, welche denen in der Testmethode entsprechend formulierten Bedingungen genügen.

Test: DocumentFactorytests
Getestete Methoden: Alle öffentlichen Methoden der Klasse DocumentFactory
Testbeschreibung: Es wird neues User Objekt erzeugt. Es wird ein vorbereitetes PolicySet aus dem Dateisystem geladen. Es wird eine Rule mit vorher festgelegten Daten erstellt. Die-

se Rule wird dem PolicySet hinzugefügt. Das PolicySet wird neu sortiert. Es wird mittels dieses PolicySet und des Benutzers eine Einwilligungserklärung im CDA Format erzeugt und in das lokale Dateisystem. Die Darstellung in Form eines PDFs wird in das lokale Dateisystem geschrieben. Es wird jeweils ein MD5 Hash für das CDA Dokument und das PolicySet erzeugt. Es werden die in ISIS vorhandenen Dokumententypen aus dem Dateisystem geladen.
Die Methoden deleteUnclearedConsent() und storeUnclearedConsent() können nur aus dem Kontext des laufenden Servers getestet werden, da sie innerhalb des working directory des Servers Lese- und Schreibvorgänge vornehmen und diese Pfadangabe erst im Betrieb des Servers aus dem Kontext abfragen.
Erfolgsbedingungen: Alle Methoden liefern die erwarteten Rückgaben, welche den der Testmethode entsprechend formulierten Bedingungen genügen. Die erstellten Dokumente wurden manuell auf ihre Richtigkeit hin überprüft.

Test: Shippertests
Getestete Methoden: Alle öffentlichen Methoden der Klasse Shipper
Testbeschreibung: Es wird neues User Objekt erzeugt. Dieser Benutzer wird im MPI registriert. Es wird die Existenz des Benutzers im MPI abgefragt. Es wird eine Einwilligungserklärung erzeugt und diese an den Consent Manager gesendet. Es wird das PolicySet der soeben gesendeten Einwilligungserklärung aus dem Consent Manager abgefragt. Es wird das PDF, das in der Einwilligungserklärung enthalten war, abgefragt und zur Überprüfung in das lokale Dateisystem geschrieben. Es wird die Liste der Einwilligungserklärungen des Benutzers abgefragt. Es wird das PDF der Einwilligungserklärung über die in der Liste enthaltenen Informationen aus dem Consent Manager abgefragt und zur Überprüfung in das lokale Dateisystem geschrieben. Es wird der Baum der an ISIS teilehmenden Organisationen von PORS abgefragt. Es wird eine Email deren Inhalt Informationen bezüglich der Wiedererlangung eines Passwortes sind an den Benutzer gesendet. Es wird ein MD5 Hash zusammen mit der ID des Benutzers an den Consent Manager geschickt. Es wird eine Aufforderung an den Consent Manager geschickt diese Informationen zu verwerfen. Der MD5 Hash wird erneut geschickt. Die unsignierte Einwilligungserklärung wird zusammen mit der ID des Benutzers an den Consent Manager geschickt. Es wird das PolicySet dieser Einwilligungserklärung aus dem Consent Manager abgefragt.
Erfolgsbedingungen: Alle Methoden liefern die erwarteten Rückgaben, welche denen in der Testmethode entsprechend formulierten Bedingungen genügen.

7.2 Oberflächentest

Das Testen der Oberfläche des Consent Creators erfolgte systematisch entsprechend der Formulierungen der Use Cases bis keine Fehler mehr auftraten und das Ergebnis den Erwartungen entsprach.

8 Diskussion und Ausblick

Das Thema Einwilligungsmanagement ist im Hinblick auf den Aufbau einer einrichtungsübergreifenden Patientenakte ein sehr bedeutendes Thema im Bereich des Gesundsheitswesens und der medizinischen Informatik.

Die in Kapitel 2.5 beschriebenen bisher umgesetzten Lösungen eines Einwilligungsmanagements zeigen jedoch Schwächen auf. Der Ansatz von [Caumanns 2008] ist technisch sehr schwer realisierbar und ebenso komplex, eine zeitnahe Umsetzung scheint nicht realistisch. Die Einwilligungserklärung wird im Ansatz von [Namli und Dogac 2006] über einen sogenannten Consent Editor erstellt. Dieser bietet jedoch nur grobe Konfigurationsmöglichkeiten. Man kann beispielsweise entweder keinen oder nur alle Ärzte vom Zugriff auf die Daten eines Patienten ausschließen. Das Konzept dieses Ansatzes ist daher nur bedingt tauglich die Vorgaben des Patienten hinsichtlich des Zugriffes auf seine Daten umzusetzen. Eine weitere Schwachstelle dieses Ansatzes ist die Abwesenheit einer Möglichkeit die erstellte Einwilligungserklärung rechtssicher entweder zu unterschreiben oder mit einer elektronischen Signatur zu versehen.

Wie der Ansatz von [Namli und Dogac 2006] basiert das entwickelte Konzept der Einwilligungserklärungen auf XACML und dem IHE BPPC Profil. Im Gegensatz zu [Namli und Dogac 2006] bietet der entwickelte Consent Creator die Möglichkeit, die erstellte Einwilligungserklärung in einem Dokument menschenlesbar anzuzeigen. Teil der Implementierung war auch die Progammierung der Möglichkeit der Versehung der Einwilligungserklärungen mit einer elektronischen Signatur. Dies steht im Kontrast zum Consent Editor, welcher weder eine Möglichkeit der schriftlichen noch elektronischen Signatur bietet. Durch das um den deny-based PEP entwickelte Konzept dieser Arbeit werden keine zusätzlichen Datenschutzregeln für die Einwilligung des Patienten benötigt, sollte eine neue Einrichtung ISIS beitreten. Die Einwilligungserklärungen des Consent Creators können XACML-Regeln auf Einrichtungsebene formulieren mit denen einzelnen Einrichtungen gezielt der Zugriff erlaubt und anderen verwehrt wird. Der Ansatz von [Namli und Dogac 2006] bietet nur die Möglichkeit einzelne Personengruppen ganzheitlich auszuschließen, eine differenzierte Auswahl einzelner Betroffener ist nicht möglich.
Das in dieser Arbeit entwickelte Konzept zur Erstellung der Einwilligungserklärungen bietet die Möglichkeiten den Zugriff bis auf Dokumenten und Personenebene zu regulieren. Die in [Birkle 2009b] beschriebene n*n Matrix von Zugriffsregeln eines idealen Einwilligungsmanagements für dieses Szenario wird dabei durch die Nutzung einer Baumstruktur von Zugriffsregeln jedoch vermieden. Ebenso müssen die Einwilligungserklärungen nicht in einer statischen und nicht anpassbaren Form vorgehalten werden, welche immer neue Anpassungen erfordern würde, sondern werden dynamisch erzeugt.

8.1 Diskussion der Methoden

Die angewendeten Methoden und Werkzeuge erwiesen sich als adäquat. Lediglich bei der Wahl der Oberfläche des Webservices wurde durch mangelnde Kommunikation mit dem ISIS-Betreiber ein Fehler begangen. Der Betreiber wurde nicht hinreichend auf die Lizenz des gewählten ExtJS hingewiesen. In Folge dessen musste der entwickelte Prototyp verworfen werden, da die GPL Lizenz unter der ExtJS verfügbar ist, nicht mit der vom Betreiber gewünschten Apache 2.0 Lizenz kompatibel ist.
Die Anforderungen an den Consent Creator wurden durch das Wasserfallmodell mit Rücksprungmöglichkeiten iterativ erfasst und es konnten sich aus den erfassten Anforderungen ergebende, neue Anforderungen in den Zielen der Implementierung berücksichtigt werden.

8.2 Diskussion der Ergebnisse

Ausgehend von den Zielen dieser Arbeit ergaben sich einige Probleme. Die geforderte optimale Lösung zur Speicherung der Einwilligungserklärungen wurde nur teilweise erreicht. Die Einwilligungserklärung wird zwar in einem an das BPPC Profil angelehnten Format gespeichert, durch die Erweiterung dieses Profils geht allerdings die Standardkonformität verloren. Gründe hierfür sind das im CDA Dokument zu speichernde PolicySet und der Text der Einwilligungserklärung, welcher für die Transformation in ein menschenlesbares Format benötigt wird. Der Text der Einwilligungserklärung selbst ist dabei in der gespeicherten Form durch Markup zwar strukturiert, nicht jedoch standardisiert. Die erstellte Einwilligungserklärung orientiert sich am Text der bisherigen Einwilligungserklärung mit der Patienten ihre Teilnahme an ISIS dokumentieren, es ist möglicherweise nicht möglich diese Einwilligungserklärung, aufgrund der jeweiligen Landesdatenschutzgesetze, in dieser Form in anderen Bundesländern zu nutzen. Dies macht Anpassungen in diesem Punkt nötig, sollte ein Betrieb des Consent Creators außerhalb von ISIS angestrebt werden.
Das entwickelte Konzept der Datenschutzregeln der Einwilligungserklärungen ermöglicht zwar die Formulierung von Datenschutzregeln bis auf Personen- und Dokumentenebene, da VPA zum Zeitpunkt dieser Arbeit nicht in der Lage ist eine Liste der Dokumente eines einzelnen Patienten zur Verfügung zu stellen, musste auf eine Implementierung dieser Funktionalität verzichtet werden. Die Datenschutzregeln können nur bis auf die Dokumentengruppenebene formuliert werden. Ebenso musste auf die Möglichkeit der Formulierung von Datenschutzregeln auf Personenebene verzichtet werden, da die zugreifenden Personen momentan nicht eindeutig identifizierbar sind, sondern nur anhand der Einrichtung aus der sie zugreifen.
Die für die Darstellung der an ISIS teilnehmenden Organisationen genutzte Implementierung eines Baums mit selektierbaren Blättern ist nur unter der LGPL v2.1 Lizenz verfügbar. Um den CC unter der, vom ISIS-Betreiber gewünschten, Apache 2.0 Lizenz verfügbar zu

machen wäre es nötig, den Baum durch eine eigene Implementierung zu ersetzen.
Das Rechtemanagement der Implementierung des Webservices bietet nur die grundlegendsten Funktionen. Die Benutzer werden lediglich in drei Klassen eingeteilt, die in der Implementierung der Oberfläche implizit Zugriff auf die Funktionen erhalten. Eine Prüfung, ob der Benutzer explizit das Recht hat diese Funktion zu nutzen findet nicht statt, es wird lediglich geprüft ob er in einer Rolle angemeldet ist, welche Zugriff auf diese Funktion besitzt. Dies macht eine differenziertere Verwaltung der zur Verfügung stehenden Funktionen momentan nicht möglich.
Aufgrund des Funktionsumfangs des CC mussten viele Details erarbeitet werden um die Abläufe der Use Cases sinnvoll zu gestalten. Zudem war es nötig die erarbeiteten rechtlichen Rahmenbedingungen zu berücksichtigen und diese in Einklang mit einer benutzerfreundlichen Bedienbarkeit zu bringen. Entsprechend zeitintensiv gestaltete sich die Implementierung, häufige Rücksprachen über geplante Umsetzung mit dem ISIS-Betreiber waren nötig.

Alle Benutzergruppen erhalten direkte Rückmeldung über den Erfolg oder Misserfolg ihrer Anfragen an den CC. Diese Rückmeldungen beschränken sich momentan darauf lediglich in knappen Worten den Grund für das Ergebnis zu schildern. In Fällen in denen Patienten von Entscheidungen der Leistungserbringer oder Administratoren betroffen sind, beispielsweise wenn eine schriftlich eingesendete Einwilligungserklärung nicht akzeptiert wurde, gibt es momentan keine Rückmeldung an den betroffenen Patienten. Aufgrund des Funktionsumfangs der Implementierung des CC wurde aus Zeitgründen drauf verzichtet.
Aus Zeitgründen wurde auch der Ablauf der Use Cases der Benutzergruppen Leistungserbringer und Administrator so formuliert, dass diese erst nach der Ausführung der eigentlich Funktion des jeweiligen Use Cases eine entsprechende Einwilligungserklärung signieren müssen, die diesen Vorgang dokumentiert. Dies sollte in Zukunft restriktiver gehandhabt werden. Eine Ausführung der gewünschten Funktion sollte erst bei vorliegen einer verbindlichen Einwilligungserklärung stattfinden.
Da zu den Benutzergruppen des CC auch die Gruppe der Patienten gehört, war es wichtig, in die Konzeption der Oberfläche die Bedürfnisse dieser Benutzergruppe einzubeziehen. Entsprechend wurde darauf geachtet die Menuführung einfach und die Darstellung verständlich zu halten. Der Patient sollte stets schnelles Feedback und Hilfe an Stellen mit komplexer Funktionalität erhalten. In die Entwicklung wurden auch Überlegungen zum Nutzungsverhalten einbezogen. Da in Übereinstimmung mit dem ISIS-Betreiber davon ausgegangen werden kann, dass Patienten nicht für jede Organisation Datenschutzregeln festlegen wollen, sondern eher groben Zugriff für einzelne Organisationen zulassen, einige Dokumente jedoch davon ausschließen wollen, bietet das entwickelte Konzept dem Patienten alle Möglichkeiten seine Vorgaben für eine Einwilligungserklärung schnell und intuitiv durch die Formulierung einer geringen Anzahl an Datenschutzregeln umzusetzen.

Der CC selbst stellt den Patienten in den Vordergrund, er bietet Patienten alle Möglichkeiten ihre Teilnahme nach ihren Vorstellungen zu gestalten und auch zu beenden. Durch die Möglichkeit eine Einwilligungserklärung selbst, ohne das zuteil tun des Leistungserbringers, zu erstellen und diese nach seinen Vorgaben formulieren zu können, stehen tatsächlich seine Interessen im Mittelpunkt. Ebenso kann er, ohne sich gegeben über dem Leistungserbringer rechtfertigen zu müssen, seine Teilnahme selbst beenden.

Das Personal der Leistungserbringer hat im Rahmen dieser Arbeit über die ihm zur Verfügung gestellten Funktionalitäten alle Möglichkeiten erhalten die Benutzer des Consent Creator effektiv zu administrieren. Die implementierten Funktionen bieten ein abgerundetes Bild, alle direkt aus der Anforderungsanalyse geforderten Funktionen wurden berücksichtigt. Die wichtigsten Funktionen bleiben der Benutzergruppe der Administratoren vorbehalten, da nur diese das entsprechende Vertrauen des ISIS-Betreibers genießen oder über die benötigten Informationen verfügen um eine qualifizierte Entscheidung zu treffen.

Die Wahlmöglichkeit zwischen der Form der elektronischen und schriftlichen Signatur ermöglicht es sowohl normalen, als auch technisch versierten Benutzern, eine Einwilligungserklärung über den CC zu erstellen und diese nach dem gewählten Verfahren zu signieren. Durch die Möglichkeit der Wahl der Methode werden keine Benutzer von der Nutzung des CC ausgeschlossen.

Durch den modularen Aufbau des CC ist es einfach möglich diesen anzupassen. Konfigurationseinstellungen wurden in XML Dateien abgelegt und können einfach ohne Änderung des Codes der Implementierung ausgetauscht werden können. Ebenso wurde bei der Implementierung der Oberfläche auf leichte Austauschbarkeit geachtet, durch den Wechsel des CSS kann jeder Betreiber sein eigenes Layout einbinden. Die Schnittstellen zum Consent Manager basieren auf HL7. Sie sind somit standardkonform und gewährleisten die geforderte Interoperabilität.

Die Implementierung bietet alle benötigten Funktionen zur effektiven Administration, die Wahl der Signatur bietet für alle Benutzer eine Möglichkeit zur Erstellung einer personalisierten Einwilligungserklärung. Die rechtssichere, elektronische Speicherung der Einwilligungserklärungen wurde erreicht.
Der Consent Creator erfüllt alle gesetzten Ziele dieser Arbeit.

8.3 Ausblick

Der Consent Creator in seiner jetzigen Form besitzt Ecken und Kanten, besonders die genutzte Implementierung des Baumes und das Rechtemanagement fallen hier auf. Die diskutierten Unzulänglichkeiten sollten in zukünftigen Versionen behoben werden.

Für die weitere Entwicklung des Consent Creators sollte ein Rollen-basiertes Rechtemanagement implementiert werden um die, dann vergrößerte, Anzahl an Funktionalitäten differenzierter zuweisen zu können. Mit der Einführung der De-Mail[24] könnte es zudem möglich sein, auch gescannte, handschriftlich unterschriebene Einwilligungserklärungen von Email-Profilen akkreditierter Anbieter zu akzeptieren, eine entsprechende Prüfung der Rechtslage vorausgesetzt. Die De-Mail ist ein Email-Verfahren das verschlüsselte Kommunikation zwischen den Email-Providern ermöglicht. Zudem werden gesicherte Anmeldeverfahren zum Zwecke der Authentizität genutzt. Die Nutzung dieses Verfahrens könnte möglich sein, da die De-Mail die Identität der Kommunikationspartner einwandfrei belegen und Veränderungen am Inhalt der Email ausschließen kann ([De-Mail 2010]).
Die erstellten Einwilligungserklärungen selbst könnten durch die Implementierung einer Möglichkeit zur Abfrage von Dokumentenlisten der Patienten von VPA zusätzlich an Mächtigkeit gewinnen. Eine Identifizierung einzelner Personen der Leistungserbringer und eine Zurverfügungstellung dieser Informationen für den Consent Creator könnte zudem Einwilligungserklärungen auf Personenebene ermöglichen. Die Standardisierung des rechtlich verbindlichen Texts der Einwilligungserklärung wäre ein weiterer Schritt in Richtung Standardkonformität des Consent Creators. Eine Internationalisierung könnte dem Consent Creator darüberhinaus ein noch größeres Anwendungsgebiet ermöglichen.

[24] *http://www.cio.bund.de/cln_102/DE/IT-Projekte/De-Mail/demail_node.html*

A Glossar

C

confidentialityCode - Siehe Kapitel 2.3.4. S,16

Consent Manager - Der CM beschränkt den Zugriff auf die Dokumente der Patienten durch die Verarbeitung der PolicySets, die in einer eigenen Datenbank vorgehalten werden. Die vom CC erhaltenen Einwilligungserklärungen werden ebenfalls im CM vorgehalten. Der CM stellt ein Interface für Anfragen bezüglich Patientendokumenten aus den beteiligten Organisationen zur Verfügung und entscheidet unter Zuhilfenahme der PolicySets, ob der Zugriff gewährt wird.

D

Datenschutzregel - Eine Datenschutzregel beschreibt den Zugriff auf eine Ressource, im Weiteren ein Dokument(e), für eine Person oder Personengruppe. Eine Datenschutzregel entspricht einer Rule eines XACML PolicySets. Die Rule kann zwei Ergebnisse haben, permit oder deny.

E

Einwilligungserklärung - Dokument, das rechtlich verbindlich die Teilnahme an ISIS regelt und den Willen des Patienten durchsetzt. Die Einwilligungserklärung ist ein CDA Dokument, welches das BPPC Profil1 implementiert und gegebenenfalls erweitert. Das Dokument beinhaltet den Rechtstext, der die Basis für die Teilnahme an ISIS bildet. Zusätzlich sind die dynamischen Datenschutzregeln, welche durch den Patienten definiert werden können, enthalten. Das CDA Dokument besteht aus der Einwilligungserklärung in menschenlesbarer Form, als XML Struktur, den Datenschutzregeln in Form eines XACML PolicySets und der Einwilligungserklärung als PDF. Das CDA Dokument ist mit einer qualifizierten elektronischen Signatur zu versehen.

EventCodeList - Beschreibt Schlüsselworte die für den Consumer einer IHE XDS Registry relevant sein können. Beinhaltet Informationen aus allen Bereichen eines CDA Dokumentes [IHE 2009a S,24].

M

Markup - Auszeichnungssprache, Begriff für die Struktur eines Dokumentenformates sowie teilweise Beschreibung des Verfahrens welches zur Verarbeitung des Formates der Daten benötigt wird.

N

Null-Einwilligung - Eine Einwilligung die den Zugriff auf die Dokumente eines Patienten verbietet und das Einstellen neuer Dokumente verhindert.

O

OID - Object Identifier, eine OID ist ein eindeutiger Identifikator eines Objektes. Siehe http://www.oid-info.com/

Opt-In - Das Opt-In Verfahren beschreibt den Vorgang der expliziten Einwilligung eines Patienten zu einem Vorgang, bespielsweise einer Operation oder der Verarbeitung seiner Daten.

P

Policy - Eine XACML Policy enthält eine oder mehrere Rules. Siehe Datenschutzregel.

PolicySet - Ein XACML PolicySet ist ein Dokument, das alle Datenschutzregeln eines Patienten enthält und genutzt wird um den Zugriff für alle Dokumente dieses Patienten zu beschränken. Das PolicySet besteht aus einer oder mehreren Policies.

X

XDS Affinity Domain - Eine XDS Affinity Domain ist eine administrative Struktur welche aus einem gut durchdachten Set von Document Source Akteuren, Document Repositories und Document Consumern besteht die sich darauf geeinigte haben Dokumente zur Verfügung zu stellen und diese in einem einzigen Document Registry Akteur zu organisieren [IHE 2009a S,89].

B Modellierung

B.1 Use Cases

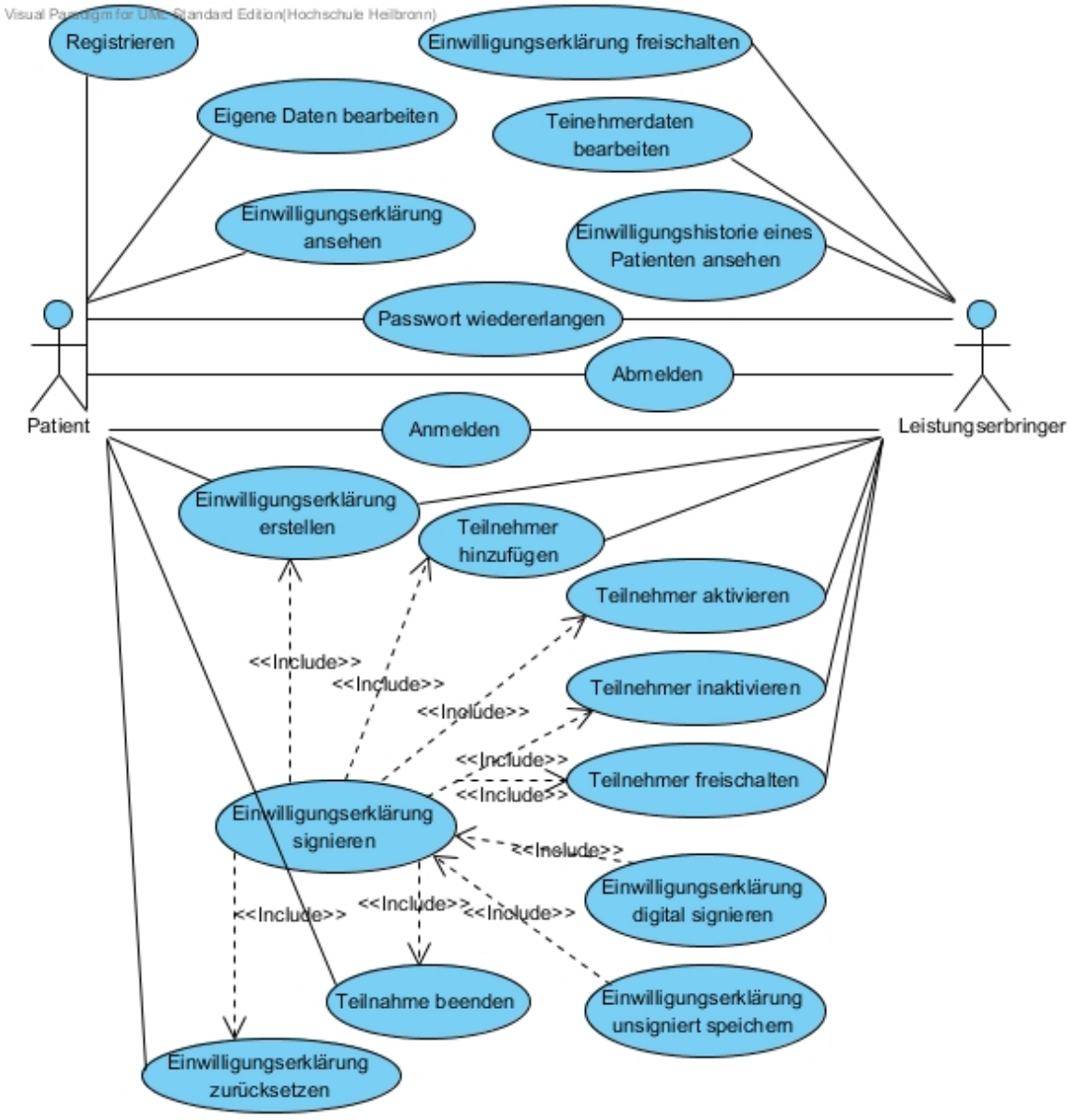

Abbildung 22: Use-Case-Diagramm

Use Case - Abmelden

Name des Use Case
Abmelden

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu der jeweiligen Rolle wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Abmelden“ aus.
2. Der Client sendet einen entsprechende Anfrage an den Server.
3. Der Consent Creator meldet den Benutzer ab.
4. Der Consent Creator zeigt dem Benutzer die Startseite an.

Normalergebnis
Der Benutzer ist im Consent Creator abgemeldet.

Alternativablauf
3a1. Das Abmelden schlägt fehl.
3a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Hauptmenu des Consent Creators an.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Anmelden

Name des Use Case
Anmelden

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen
-

Normalablauf
1. Der Benutzer ruft den Consent Creator auf.
2. Der Consent Creator zeigt dem Benutzer clientseitig das Hauptmenu-Menu an.
3. Der Benutzer wählt die Funktion „Anmelden aus“.
4. Der Consent Creator zeigt dem Benutzer clientseitig das Anmelde-Menu an.
5. Der Benutzer gibt seine Anmelde-Daten ein.
6. Der Benutzer wählt die Funktion „Anmelden“ aus.
7. Der Client sendet die Anmeldeinformationen an den Consent Creator.
8. Der Consent Creator meldet den Benutzer unter den eingegebenen Daten an.
9. Der Consent Creator zeigt dem Benutzer das Hauptmenu des Consent Creators, gemäß der Privilegien des Benutzers.

Normalergebnis
Der Benutzer ist im Consent Creator angemeldet.

Alternativablauf
8a1. Das Anmelden schlägt fehl, der Benutzer erhält eine Mitteilung, die dies besagt.
8a2. Die Darstellung zeigt weiter das Anmelde-Menu.

Nicht funktionale Anforderungen
-

Notiz
Das Anmelden wird auch dann als fehlgeschlagen gemeldet, wenn der Benutzer eine falsche Emailaddresse/Passwort-Kombination angibt.

Use Case - Eigene Daten bearbeiten

Name des Use Case
Eigene Daten bearbeiten

Subsystem
Consent Creator

Aktoren
Patient

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Patienten wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Eigene Daten bearbeiten“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator stellt die Informationen des Patienten dar.
4. Der Benutzer editiert seine Daten gemäß seiner Wünsche.
5. Der Benutzer bestätigt seine Angaben.
6. Der Client sendet eine Anfrage, in der die neuen Daten des Patienten enthalten sind, an den Consent Creator.
7. Der Consent Creator ändert die Daten des Patienten.
8. Der Consent Creator sendet eine Rückmeldung an den Patienten.

Normalergebnis
Der Patient hat seine Daten geändert.

Alternativablauf
7a1. Die Änderung schlägt fehl.
7a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Eingabe der Änderungen an.

Nicht funktionale Anforderungen
-

Notiz

-

Use Case - Einwilligungserklärung ansehen

Name des Use Case
Einwilligungserklärung ansehen

Subsystem
Consent Creator

Aktoren
Patient

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Patienten wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Einwilligungserklärung einsehen“ aus.
2. Der Client sendet eine Anfrage, in dem die aktuelle Einwilligungserklärung des Patienten angefordert wird, an den Consent Creator.
3. Der Consent Creator fragt die Einwilligungserklärung in Form eines PDFs aus dem Consent Manager ab.
4. Der Consent Creator stellt die Einwilligungserklärung dem Benutzer zur Verfügung.

Normalergebnis
Die Einwilligungserklärung wird dem Benutzer angezeigt.

Alternativablauf
3a1. Die Einwilligungserklärung konnte nicht abgefragt werden.
3a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Hauptmenu an.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Einwilligungserklärung digital signieren

Name des Use Case
Einwilligungserklärung digital signieren

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet und will eine Einwilligungserklärung erstellen.
Der Benutzer hat die Einwilligungserklärung in Form eines PDFs zur Ansicht erhalten.

Normalablauf
1. Der Consent Creator öffnet auf dem Client das Menu zur digitalen Signierung einer Einwilligungserklärung.
2. Der Benutzer wählt die für die Signierung benötigte Treiberdatei seines Kartenlesers aus.
3. Der Benutzer gibt seine PIN ein, um die Signierung der Dokumente durch die sichere Signaturerstellungseinheit zu ermöglichen.
4. Der Benutzer wählt die Funktion „Signieren“ aus.
5. Der Client signiert die Einwilligungserklärung im CDA Format, welche vom Consent Creator abgefragt wird.
6. Der Client sendet das signierte Dokument an den Consent Creator.
7. Der Consent Creator teilt dem Benutzer die erfolgreiche Signierung mit.
8. Der Consent Creator sendet die Einwilligungserklärung als CDA Dokument an den Consent Manager.
9. Der Consent Creator meldet dem Benutzer die erfolgreiche Speicherung der Einwilligungserklärung.

Normalergebnis
Die Einwilligungserklärung des Benutzers wurde signiert.

Alternativablauf
5a1. Die Angaben des Benutzers lassen keine Signierung zu.
5a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Signierung einer Einwilligungserklärung an.

5b1. Die Signierung schlägt systemintern fehl.
5b2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Signierung einer Einwilligungserklärung an.

6a1. Die Übertragung der Dokumente schlägt fehl.
6a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Signierung einer Einwilligungserklärung an.

8a1. Das Versenden der Einwilligungserklärung schlägt fehl.
8a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Menu zur Erstellung einer Einwilligungserklärung an.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Einwilligungserklärung erstellen

Name des Use Case
Einwilligungserklärung erstellen

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Einwilligungserklärung erstellen“ aus.
2. Der Client sendet eine Anfrage bezüglich des Menus zur Erstellung einer Einwilligungserklärung an den Server.
3. Der Consent Creator öffnet das Menu zur Einwilligungserstellung auf dem Client und

sendet die für die Darstellung benötigten Informationen.
4. Der Benutzer sieht eine Darstellung der Datenschutzregeln seiner bisher gültigen Einwilligungserklärung.
5. Der Benutzer entfernt, ändert oder fügt neue Datenschutzregeln hinzu.
6. Der Benutzer wählt die Funktion „Einwilligungserklärung speichern“ aus.
7. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
8. Der Consent Creator erstellt die Einwilligungserklärung als PDF und CDA Dokument.
9. Der Consent Creator stellt dem Benutzer das PDF zur Ansicht zur Verfügung.
10. Der Consent Creator fordert den Benutzer gemäß Use Case „Einwilligungserklärung signieren“ auf, die Einwilligungserklärung zu signieren.
11. Der Consent Creator meldet dem Benutzer die erfolgreiche Speicherung der Einwilligungserklärung.

Normalergebnis
Die Einwilligungserklärung wurde erfolgreich gespeichert.

Alternativablauf
2a1. Der Benutzer ist als Leistungserbringer angemeldet.
2a2. Der Consent Creator zeigt dem Benutzer das Menu zur Suche eines Teilnehmers an.
2a3. Der Benutzer gibt die Stammdaten des Teilnehmers ein.
2a4. Der Benutzer wählt die Funktion „Suchen“ aus.
2a5. Der Client sendet die Stammdaten an den Consent Creator.
2a6. Der Consent Creator sucht den Teilnehmer gemäß der Stammdaten und zeigt diese dem Benutzer clientseitig an.
2a7. Der Benutzer bestätigt die Daten.
2a7. Der Client sendet die Bestätigung an den Consent Creator.
2a8. Der Consent Creator öffnet auf dem Client das Menu zur Erstellung einer Einwilligungserklärung für den gesuchten Patienten.
2a9. Der Benutzer sieht eine Darstellung der Datenschutzregeln der bisher gültigen Einwilligungserklärung des gesuchten Patienten.
2a10. Weiter mit Normalablauf 5.

10a1. Die Signierung der Einwilligungserklärung war nicht erfolgreich.
10a2. Der Consent Creator teilt dies dem Benutzer mit und speichert die Einwilligungserklärung nicht.
10a3. Die Darstellung zeigt weiter das Signierungs-Menu.

Nicht funktionale Anforderungen

-

Notiz
-

Use Case - Einwilligungserklärung freischalten

Name des Use Case
Einwilligungserklärung freischalten

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Leistungserbringer wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Einwilligungserklärung freischalten“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator stellt auf dem Client die Informationen über gespeicherte, unsignierte Einwilligungserklärungen dar.
4. Der Benutzer wählt die Funktion „Einwilligungserklärung freischalten“ aus.
5. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
6. Der Consent Creator lädt die Einwilligungserklärung aus dem Dateisystem und sendet diese an den Consent Manager.
7. Der Consent Creator löscht die Einwilligungserklärung aus dem Dateisystem des Consent Creators.
8. Der Consent Creator löscht den entsprechenden Eintrag über die unsignierte Einwilligungserklärung in der Datenbank.
9. Der Consent Creator teilt dem Benutzer die erfolgreiche Freischaltung der Einwilligungserklärung mit.

Normalergebnis
Die Einwilligungserklärung wurde freigeschaltet.

Alternativablauf
4a1. Der Benutzer wählt die Funktion „Einwilligungserklärung ablehnen“ aus.
4a2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
4a3. Der Consent Creator löscht die im Dateisystem des Consent Creators gespeicherte Einwilligungserklärung.
4a4. Der Consent Creator löscht den entsprechenden Eintrag aus der Datenbank.
4a5. Der Consent Creator sendet dem Consent Manager die Information, den zur Einwilligungserklärung dieses Patienten gespeicherten MD5 Hash zu verwerfen.
4a6. Der Consent Creator teilt dem Benutzer das erfolgreiche Löschen der Einwilligungserklärung mit.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Einwilligungserklärung signieren

Name des Use Case
Einwilligungserklärung signieren

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet und will eine Einwilligungserklärung erstellen.
Der Benutzer hat die Einwilligungserklärung in Form eines PDFs zur Ansicht erhalten.

Normalablauf
1. Der Consent Creator öffnet auf dem Client das Menu zur Signierung einer Einwilligungserklärung.
2. Der Benutzer wählt die Funktion „Digitale Signierung“ aus.
3. Der Client sendet die Auswahl an den Consent Creator.

4. Der Consent Creator öffnet auf dem Client das Menu zur digitalen Signatur einer Einwilligungserklärung.
5. Der Consent Creator fordert den Benutzer gemäß Use Case „Einwilligungserklärung digital signieren“ auf, die Einwilligungserklärung zu signieren.

Normalergebnis
-

Alternativablauf
2a1. Der Benutzer wählt die Funktion „Schriftliche Signatur“ aus.
2a2. Der Client sendet die Auswahl den Consent Creator.
2a3. Der Consent Creator öffnet auf dem Client das Menu zur schriftlichen Signatur einer Einwilligungserklärung.
2a4. Der Consent Creator fordert den Benutzer gemäß Use Case „Einwilligungserklärung unsigniert speichern“ auf, die weiteren Schritte durchzuführen.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Einwilligungserklärung unsigniert speichern

Name des Use Case
Einwilligungserklärung unsigniert speichern

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet und will eine Einwilligungserklärung erstellen.
Der Benutzer hat seine Einwilligungserklärung in Form eines PDFs zur Ansicht erhalten.

Normalablauf

1. Der Consent Creator öffnet auf dem Client das Menu zur schriftlichen Signierung einer Einwilligungserklärung.
2. Der Benutzer wählt die Funktion „Schriftliche Signatur“ aus.
3. Der Consent Creator erzeugt einen Schlüssel der die Unverfälschtheit der Einwilligungserklärung im CDA Format belegt und sendet diesen an den Consent Manager.
4. Der Consent Creator speichert die Informationen über die Wahl der schriftlichen Signatur in der Datenbank des Consent Creators, erzeugt eine ID für die Einwilligungserklärung und speichert die Einwilligungserklärung unter der generierten ID pseudonymisiert im Dateisystem des Consent Creators.
5. Der Consent Creator teilt dem Benutzer die erfolgreiche Speicherung seiner unsignierten Einwilligungserklärung mit.

Normalergebnis
Die unsignierte Einwilligungserklärung des Benutzers wurde gespeichert.

Alternativablauf
3a1. Das Versenden schlägt fehl.
3a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur schriftlichen Signierung einer Einwilligungserklärung an.

4a1. Die Vorgänge schlagen fehl.
4a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur schriftlichen Signierung einer Einwilligungserklärung an.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Einwilligungserklärung zurücksetzen

Name des Use Case
Einwilligungserklärung zurücksetzen

Subsystem
Consent Creator

Aktoren
Patient

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Patienten wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Einwilligungserklärung zurücksetzen“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator öffnet auf dem Client das Menu zu Auswahl der Form der Signatur zur Zurücksetzung der Einwilligungserklärung.
4. Der Consent Creator erstellt eine Einwilligungserklärung, die den Zugriff auf jegliche Dokumente des Patienten verwehrt, das Einstellen von Dokumenten aber weiterhin ermöglicht.
5. Der Consent Creator fordert den Benutzer auf, diese Einwilligungserklärung gemäß des Use Case „Einwilligungserklärung signieren“ zu signieren.
6. Der Consent Creator meldet dem Benutzer die erfolgreiche Zurücksetzung der Einwilligungserklärung.

Normalergebnis
Die Einwilligungserklärung des Benutzers wurde zurückgesetzt.

Alternativablauf
5a1. Die Signierung schlägt fehl.
5a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Signierungsmenu an.

Nicht funktionale Anforderungen
-

Notiz

-

Use Case - Einwilligungserklärungshistorie eines Patienten ansehen

Name des Use Case
Einwilligungserklärungshistorie eines Patienten ansehen

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Leistungserbringer wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Einwilligungshistorie einsehen“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator fordert den Benutzer auf, den Patienten dessen Einwilligungshistorie eingesehen werden soll, zu identifizieren. Hierzu öffnet sich auf dem Client ein Menu zur Eingabe von Stammdaten.
4. Der Benutzer gibt die Stammdaten des entsprechenden Patienten ein und bestätigt seine Eingabe.
5. Der Client sendet eine Anfrage mit diesen Daten an den Consent Creator.
6. Der Consent Creator sucht den Patienten und stellt die Stammdaten des Patienten auf dem Client dar.
7. Der Benutzer wählt die Funktion „Historie einsehen“ aus.
8. Der Consent Creator fragt eine Liste der Einwilligungserklärungen des Patienten aus dem Consent Manager ab.
9. Der Consent Creator übermittelt dem Client eine Liste der Einwilligungserklärungen. Diese wird dem Benutzer zur Verfügung gestellt.
10. Der Benutzer wählt eine Einwilligungserklärung aus.
11. Der Client sendet eine Anfrage, in dem diese Einwilligungserklärung angefordert wird, an den Consent Creator.
12. Der Consent Creator fragt diese Einwilligungserklärung beim Consent Manager nach.
13. Der Consent Manager sendet die Einwilligungserklärung an den Consent Creator.

14. Der Consent Creator stellt dem Benutzer die Einwilligungserklärung zur Verfügung.

Normalergebnis
Der Benutzer hat eine Sicht der Einwilligungshistorie erhalten und kann die einzelnen Dokumente einsehen.

Alternativablauf
6a1. Der Consent Creator kann den Patienten nicht finden.
6a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Eingabe der Stammdaten an.

8a1. Das Abfragen der Einwilligungserklärungen aus dem Consent Manager schlägt fehl.
8a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Eingabe der Stammdaten an.

12a1. Das Abfragen der Einwilligungserklärung aus dem Consent Manager schlägt fehl.
12a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Eingabe der Stammdaten an.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Passwort wiedererlangen

Name des Use Case
Passwort wiedererlangen

Subsystem
Consent Creator

Aktoren
Patient, Leistungserbringer

Kontext und Vorbedingungen

-

Normalablauf
1. Der Benutzer ruft den Consent Creator auf.
2. Der Consent Creator zeigt dem Benutzer clientseitig das Hauptmenu-Menu an.
3. Der Benutzer wählt die Funktion „Passwort anfordern“ aus.
4. Der Consent Creator öffnet auf dem Client das Menu zur Anforderung eines Passwortes.
5. Der Benutzer gibt seine Emailaddresse ein.
6. Der Benutzer wählt die Funktion „Passwort anfordern“ aus.
7. Der Client sendet die Emailaddresse an den Server.
8. Der Cosent Creator prüft, ob zu der übergebenen Emailaddresse ein Teilnehmer existiert.
9. Der Consent Creator sendet eine Email mit einem Link an die Emailaddresse des Teilnehmers.
10. Der Benutzer folgt dem in der Email enthaltenen Link.
11. Der Benutzer wird aufgefordert ein neues Passwort anzugeben.
12. Der Benutzer gibt sein neues Passwort ein und bestätigt seine Angaben.
13. Der Client sendet das neue Passwort an den Consent Creator.
14. Der Consent Creator ändert das für den Benutzer gespeicherte Passwort.
15. Der Consent Creator teilt dem Benutzer die erfolgreiche Änderung seines Passwortes mit.

Normalergebnis
Der Benutzer hat ein neues Passwort für sein Profil gesetzt.

Alternativablauf
8a1. Es existiert kein Benutzer mit der angegebenen Emailaddresse.
8a2. Der Benutzer erhält eine Mitteilung, die besagt, dass diese Emailaddresse unbekannt ist.

10a1. Der Benutzer folgt dem Link nicht.
10a2. Der Link verfällt nach 72 Stunden und kann nicht mehr genutzt werden.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Registrieren

Name des Use Case
Registrieren

Subsystem
Consent Creator

Aktoren
Patient

Kontext und Vorbedingungen
-

Normalablauf
1. Der Benutzer ruft den Consent Creator auf.
2. Der Consent Creator zeigt dem Benutzer clientseitig das Hauptmenu an.
3. Der Benutzer wählt die Funktion „Registrieren“ aus.
4. Der Consent Creator öffnet clientseitig das Menu zur Registrierung eines neuen Teilnehmers.
5. Der Benutzer gibt seine, zur Registrierung benötigten, Stammdaten ein.
6. Der Benutzer wählt die Funktion „Registrieren“ aus.
7. Der Client sendet die Stammdaten an den Server.
8. Der Consent Creator prüft, ob in der lokalen Datenbank bereits ein Teilnehmer unter diesen Stammdaten registriert ist.
9. Der Consent Creator prüft, ob im MPI bereits ein Teilnehmer unter diesen Stammdaten registriert ist.
10. Der Consent Creator trägt den neuen Teilnehmer in der lokalen Datenbank und im MPI ein.
11. Der Consent Creator teilt dem Benutzer die erfolgreiche Registrierung mit und sendet dem Benutzer eine Email mit einem Link über den er selbst sein Passwort setzen kann.
12. Der Consent Creator sendet dem Consent Manager eine Null-Einwilligung (Siehe Anhang A - Glossar) für diesen Patienten.

Normalergebnis
Der Benutzer ist im Consent Creator registriert.

Alternativablauf

8a1. Es existiert bereits ein Benutzer mit den angegebenen Stammdaten.
8a2. Das Registrieren wird abgebrochen.
8a3. Der Benutzer erhält eine Mitteilung, die besagt, dass zu diesen Stammdaten bereits ein Teilnehmer existiert.

9a1. Es existiert bereits ein Benutzer mit den angegebenen Stammdaten.
9a2. Das Registrieren wird abgebrochen.
9a3. Der Benutzer erhält eine Mitteilung, welche besagt, dass zu diesen Stammdaten bereits ein Teilnehmer existiert, der allerdings noch nicht im Consent Creator registriert ist. Um sich mit den entsprechenden Daten zu registrieren, möge er sich an den entsprechenden Verantwortlichen des Projektes wenden. Der Benutzer wird als inaktiver Benutzer hinzugefügt, er kann sich nicht anmelden, bis der Betreiber ihn freigeschaltet hat.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Teilnahme beenden

Name des Use Case
Teilnahme beenden

Subsystem
Consent Creator

Aktoren
Patient

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Patienten wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Teilnahme beenden“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator stellt das Menu zur Wahl der Methode der Signatur zur Beendigung der Teilnahme dar.

4. Der Benutzer kann die Einwilligungserklärung, welche seine Teilnahme beendet, ansehen. Diese Einwilligungserklärung verhindert das Einstellen neuer Dokumente und verhindert ebenso das Ansehen bereits eingestellter Dokumente.
4. Der Consent Creator fordert den Benutzer auf, die Einwilligungserklärung gemäß des Use Case „Einwilligungserklärung signieren“ zu signieren.
5. Der Consent Creator deaktiviert den Benutzer.
6. Der Consent Creator meldet den Benutzer ab.

Normalergebnis
Der Patient ist im System als inaktiv markiert. Die erstellte Einwilligungserklärung verhindert das Einstellen oder Ansehen seiner Dokumente.

Alternativablauf
5a1. Im Falle der Wahl der schriftlichen Signatur wird der Benutzer nicht deaktiviert.
5a2. Der Benutzer wird nicht abgemeldet.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Teilnehmer aktivieren

Name des Use Case
Teilnehmer aktivieren

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Leistungserbringer wird dargestellt.

Normalablauf

1. Der Benutzer ruft die Funktion „Teilnehmer aktivieren“ auf.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator fordert den Leistungserbringer auf, den aktiv zu setzenden Teilnehmer zu identifizieren und öffnet hierzu ein Menu zur Eingabe der Stammdaten des Teilnehmers.
4. Der Leistungserbringer gibt die Stammdaten des Patienten ein und bestätigt seine Angaben.
5. Der Client sendet die Stammdaten an den Consent Creator.
6. Der Consent Creator sucht den Patienten und stellt die Daten des Teilnehmers für den Benutzer dar.
7. Der Benutzer wählt die Funktion „Teilnehmer aktivieren“ aus.
8. Der Client fordert den Benutzer auf, seine Auswahl zu bestätigen.
9. Der Benutzer bestätigt seine Auswahl.
10. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
11. Der Consent Creator aktiviert den Teilnehmer.
12. Der Consent Creator meldet dem Benutzer die erfolgreiche Aktivierung des Teilnehmers.
13. Der Consent Creator erstellt eine Einwilligungserklärung, die es ermöglicht, Dokumente des Teilnehmers einzustellen, es jedoch verbietet, Dokumente anzusehen.
14. Der Consent Creator fordert den Benutzer auf, die Einwilligungserklärung gemäß des Use Case „Einwilligungserklärung signieren“ zu signieren.

Normalergebnis
Der Patient ist im System als aktiv markiert. Es ist durch die neue Einwilligungserklärung wieder möglich, Dokumente des Patienten einzustellen. Die Dokumente des Patienten können nicht eingesehen werden.

Alternativablauf
6a1. Der Patient konnte nicht gefunden werden.
6a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Menu zur Eingabe der Stammdaten.

11a1. Das Aktivieren schlägt fehl, der Benutzer erhält eine Mitteilung, die dies besagt.
11a2. Die Darstellung zeigt weiter das Menu mit der Darstellung der Stammdaten des Patienten.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Teilnehmer freischalten

Name des Use Case
Teilnehmer freischalten

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu für Leistungserbringer wird dargestellt.

Normalablauf
1. Der Benutzer ruft die Funktion „Teilnehmer freischalten“ auf.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator stellt auf dem Client eine Liste der möglichen, freizuschaltenden Teilnehmer dar.
4. Der Benutzer wählt die Funktion „Teilnehmer freischalten“ aus.
5. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
6. Der Consent Creator aktiviert den entsprechenden Benutzer in der Datenbank.
7. Der Consent Creator löscht den Eintrag über den Datenkonflikt, wegen dessen der Benutzer freigeschaltet werden musste.
8. Der Consent Creator sendet dem Patienten eine Email, um ein neues Passwort zu setzen.
9. Der Consent Creator informiert den Benutzer über die erfolgreiche Freischaltung.
10. Der Consent Creator erstellt eine Einwilligungserklärung, die es ermöglicht, Dokumente des Teilnehmers einzustellen, es jedoch verbietet, Dokumente anzusehen.
11. Der Consent Creator fordert den Benutzer auf, die Einwilligungserklärung gemäß des Use Case „Einwilligungserklärung signieren“ zu signieren.

Normalergebnis
Der Patient ist im System als aktiv markiert. Es ist durch die neue Einwilligungserklärung wieder möglich, Dokumente des Patienten einzustellen. Die Dokumente des Patienten kön-

nen nicht eingesehen werden.

Alternativablauf
4a1. Der Benutzer wählt die Funktion „Registrierung ablehnen“ aus.
4a2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
4a3. Der Consent Creator löscht den entsprechenden Datensatz aus der Datenbank.
4a5. Der Consent Creator teilt dies dem Benutzer mit.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Teilnehmer hinzufügen

Name des Use Case
Teilnehmer hinzufügen

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet. Das Hauptmenu für Leistungserbringer wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Teilnehmer hinzufügen“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
2. Der Consent Creator zeigt dem Benutzer das Menu zum Hinzufügen neuer Teilnehmer auf dem Client an.
3. Der Benutzer gibt die Stammdaten des neuen Teilnehmers ein.
4. Der Benutzer wählt die Funktion „Teilnehmer speichern“ aus.
5. Der Client sendet eine Anfrage mit den eingegebenen Stammdaten an den Consent Creator.
6. Der Consent Creator prüft die Daten.

7. Der Consent Creator erstellt einen entsprechenden Eintrag in der Benutzerdatenbank des Consent Creators und in den Verzeichnissen des MPI.
8. Der Consent Creator fordert den Benutzer auf, eine Einwilligungserklärung für den Patienten gemäß des Use Case „Einwilligungserklärung erstellen“ zu erstellen und zu signieren.

Normalergebnis
Der Teilnehmer wurde dem System hinzugefügt, eine Einwilligungserklärung wurde erstellt und signiert.

Alternativablauf
6a1. Die Überprüfung schlägt fehl oder es wird festgestellt, dass zu den angegebenen Daten bereits ein Teilnehmer existiert.
6a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Menu zum Hinzufügen eines Teilnehmers an.

7a1. Das Anlegen des neuen Profils schlägt fehl.
7a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Menu zum Hinzufügen eines Teilnehmers an.

Nicht funktionale Anforderungen
-

Notiz
-

Use Case - Teilnehmer inaktivieren

Name des Use Case
Teilnehmer inaktivieren

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen

Der Benutzer ist angemeldet, das Hauptmenu für Leistungserbringer wird dargestellt.

Normalablauf
1. Der Benutzer ruft die Funktion „Teilnehmer inaktivieren“ auf.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator fordert den Leistungserbringer auf, den inaktiv zu setzenden Teilnehmer zu identifizieren und öffnet hierzu ein Menu zur Eingabe der Stammdaten des Teilnehmers.
4. Der Leistungserbringer gibt die Stammdaten des Patienten ein und bestätigt seine Angaben.
5. Der Client sendet die Stammdaten an den Consent Creator.
6. Der Consent Creator sucht den Patienten und stellt die Daten des Teilnehmers für den Benutzer dar.
7. Der Benutzer wählt die Funktion „Teilnehmer inaktivieren“ aus.
8. Der Client fordert den Benutzer auf, seine Auswahl zu bestätigen.
9. Der Benutzer bestätigt seine Auswahl.
10. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
11. Der Consent Creator deaktiviert den Teilnehmer.
12. Der Consent Creator meldet dem Benutzer die erfolgreiche Deaktivierung des Teilnehmers.
13. Der Consent Creator erstellt eine Einwilligungserklärung, die es verbietet, Dokumente des Teilnehmers einzustellen und auf seine bereits eingestellten Dokumente zu zugreifen.
14. Der Consent Creator fordert den Benutzer auf, die Einwilligungserklärung gemäß des Use Case „Einwilligungserklärung signieren“ zu signieren.

Normalergebnis
Der Patient ist im System als inaktiv markiert. Die erstellte Einwilligungserklärung verhindert das Einstellen oder Ansehen seiner Dokumente.

Alternativablauf
6a1. Der Patient konnte nicht gefunden werden.
6a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt das Menu zur Eingabe der Stammdaten.

11a1. Das Inaktivieren schlägt fehl, der Benutzer erhält eine Mitteilung, die dies besagt.
11a2. Die Darstellung zeigt weiter das Menu mit der Darstellung der Stammdaten des Patienten.

Nicht funktionale Anforderungen

-

Notiz
-

Use Case - Teilnehmerdaten bearbeiten

Name des Use Case
Teilnehmerdaten bearbeiten

Subsystem
Consent Creator

Aktoren
Leistungserbringer

Kontext und Vorbedingungen
Der Benutzer ist angemeldet, das Hauptmenu wird dargestellt.

Normalablauf
1. Der Benutzer wählt die Funktion „Teilnehmer bearbeiten“ aus.
2. Der Client sendet eine entsprechende Anfrage an den Consent Creator.
3. Der Consent Creator fordert den Benutzer auf, den Patienten, welcher bearbeitet werden soll, zu identifizieren. Hierzu öffnet sich auf dem Client ein Menu zur Eingabe von Stammdaten.
4. Der Benutzer gibt die Stammdaten des entsprechenden Patienten ein und bestätigt seine Eingabe.
5. Der Client sendet eine Anfrage mit diesen Daten an den Consent Creator.
6. Der Consent Creator sucht den Patienten und stellt die Informationen des Patienten für den Benutzer dar.
7. Der Benutzer editiert die Daten des Patienten gemäß seiner Wünsche.
8. Der Benutzer bestätigt seine Angaben.
9. Der Client sendet eine Anfrage, in dem die neuen Daten des Patienten enthalten sind, an den Consent Creator.
10. Der Consent Creator ändert die Daten des Patienten.
11. Der Consent Creator sendet eine Rückmeldung an den Benutzer.

Normalergebnis

Der Benutzer hat die Daten des gesuchten Patienten geändert.

Alternativablauf
6a1. Der Consent Creator kann den Patienten nicht finden.
6a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Eingabe der Stammdaten an.

10a1. Die Änderung schlägt fehl.
10a2. Der Consent Creator teilt dies dem Benutzer mit und zeigt weiter das Menu zur Eingabe der Änderungen an.

Nicht funktionale Anforderungen
-

Notiz
-

B.2 Klassendiagramm

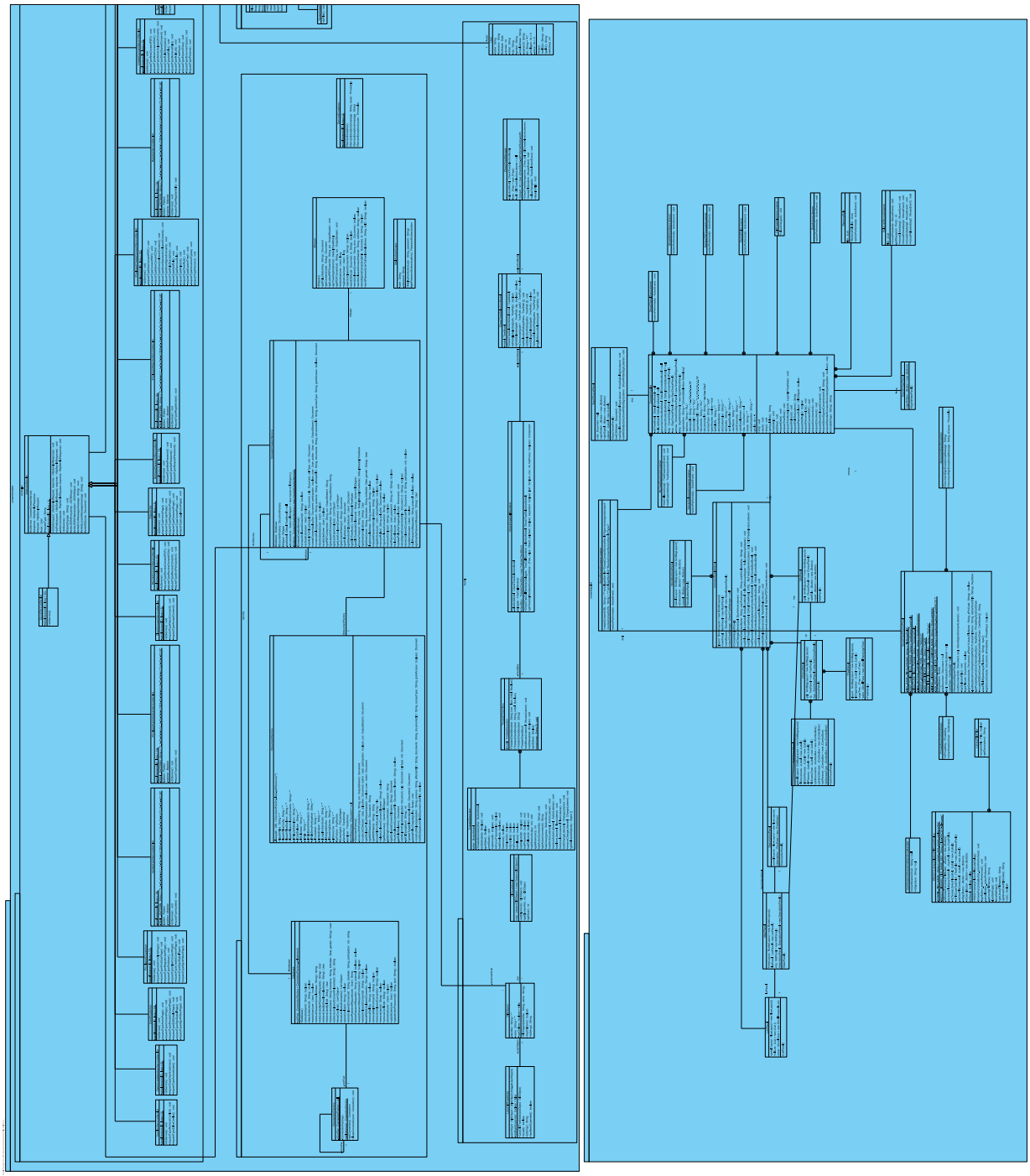

Abbildung 23: Klassendiagramm

B.3 Sequenzdiagramme

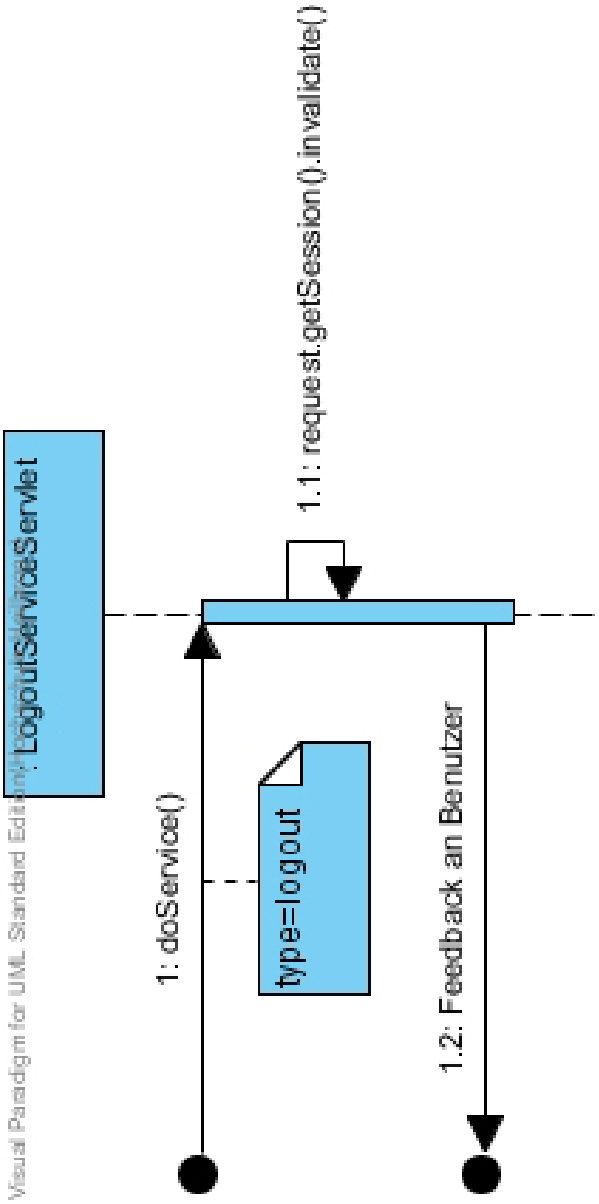

Abbildung 24: Sequenzdiagramm Use Case Abmelden

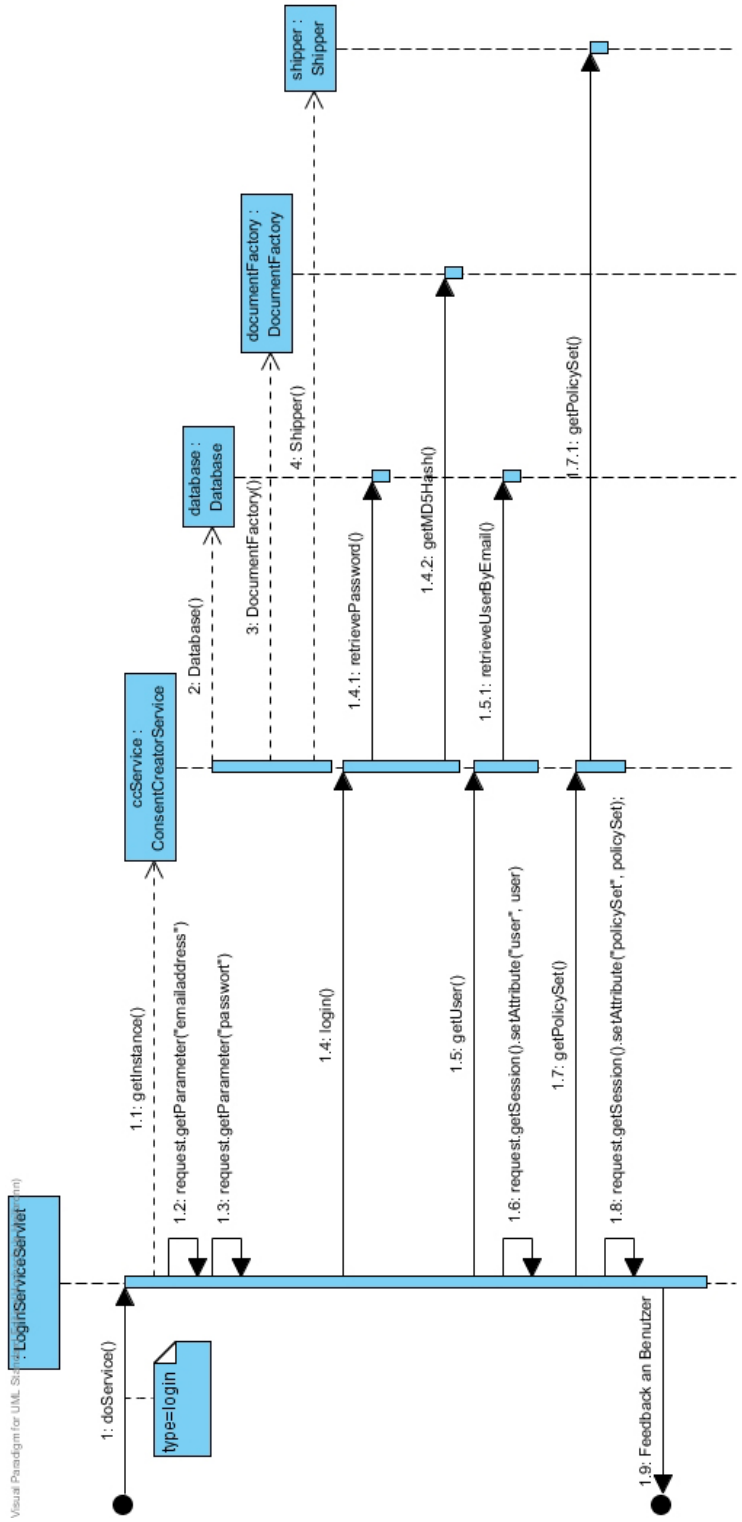

Abbildung 25: Sequenzdiagramm Use Case Anmelden

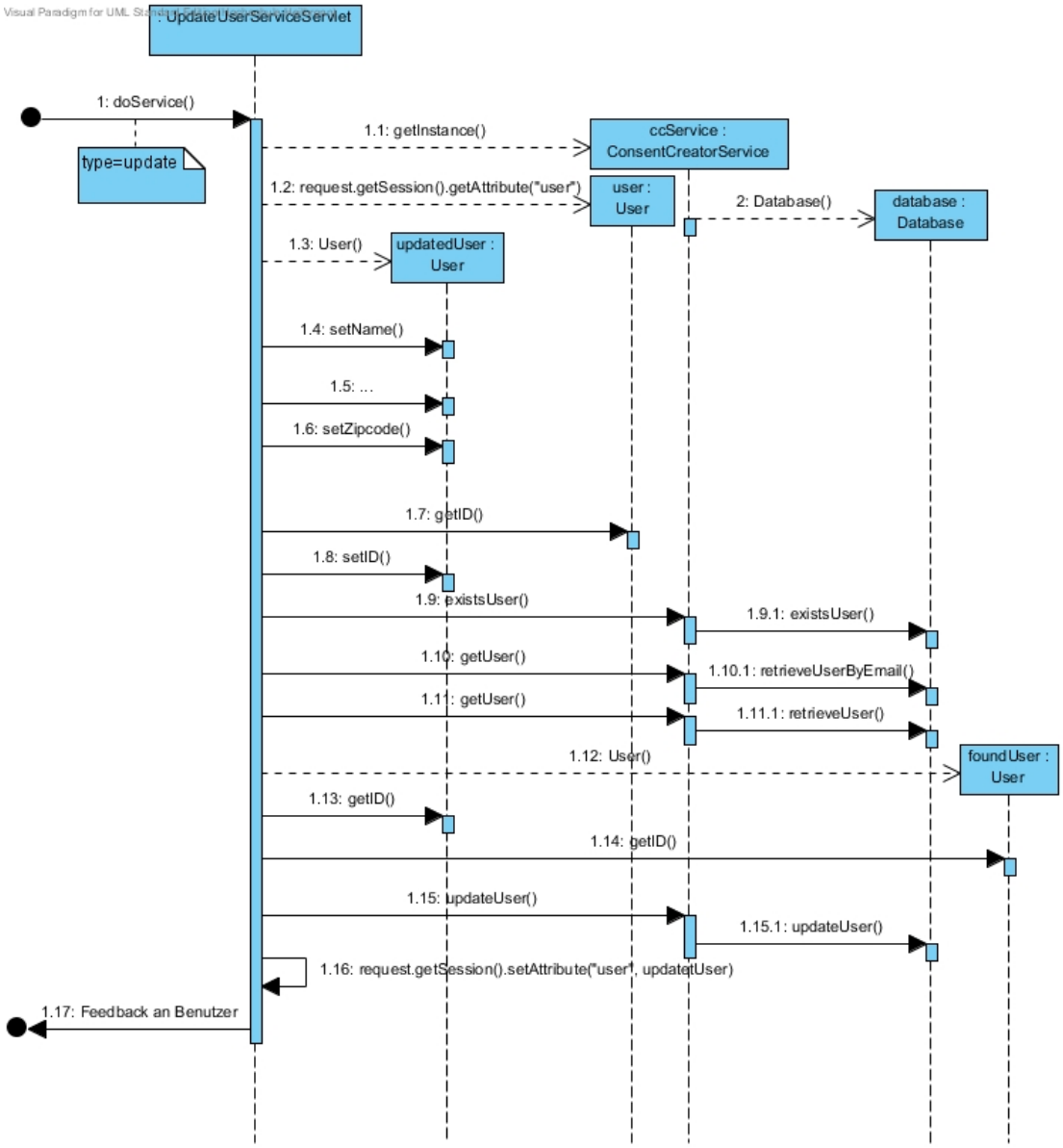

Abbildung 26: Sequenzdiagramm Use Case Eigene Daten bearbeiten

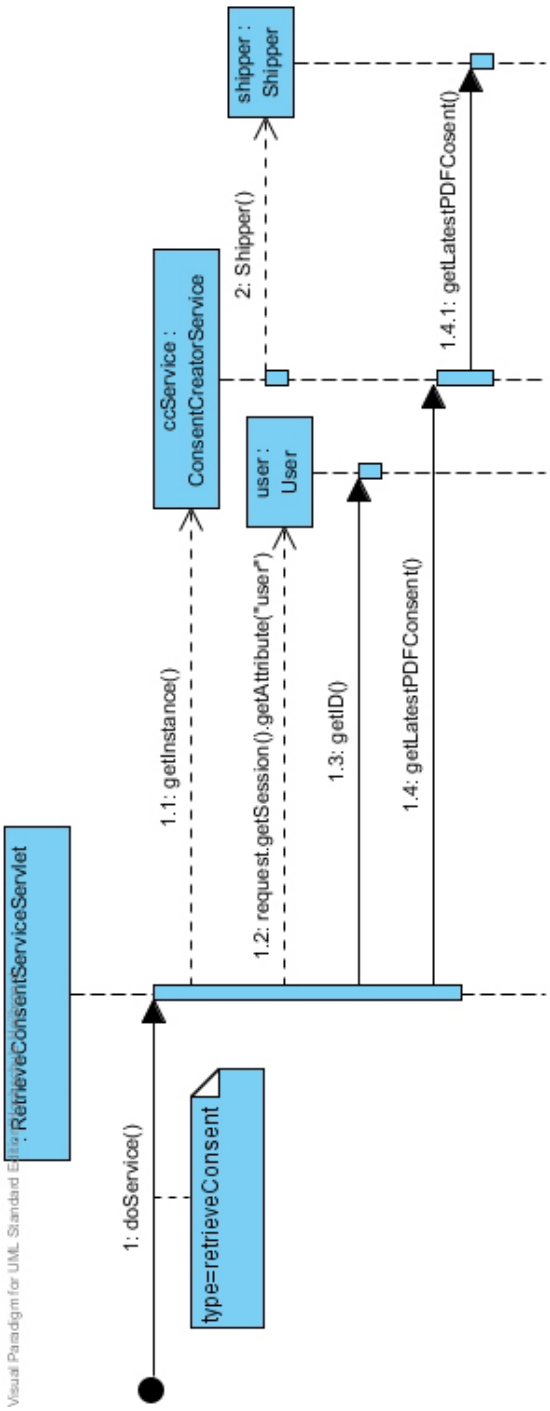

Abbildung 27: Sequenzdiagramm Use Case Einwilligungserklärung ansehen

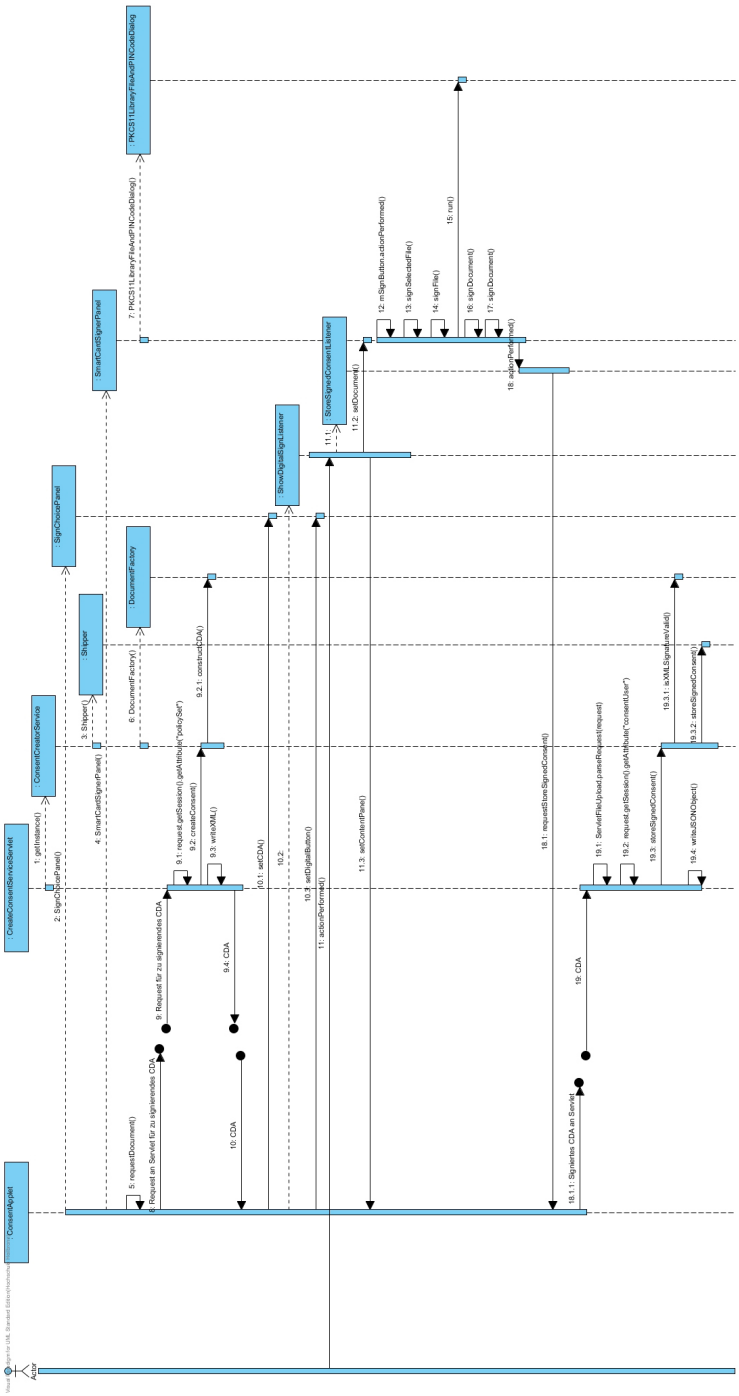

Abbildung 28: Sequenzdiagramm Use Case Einwilligungserklärung digital signieren

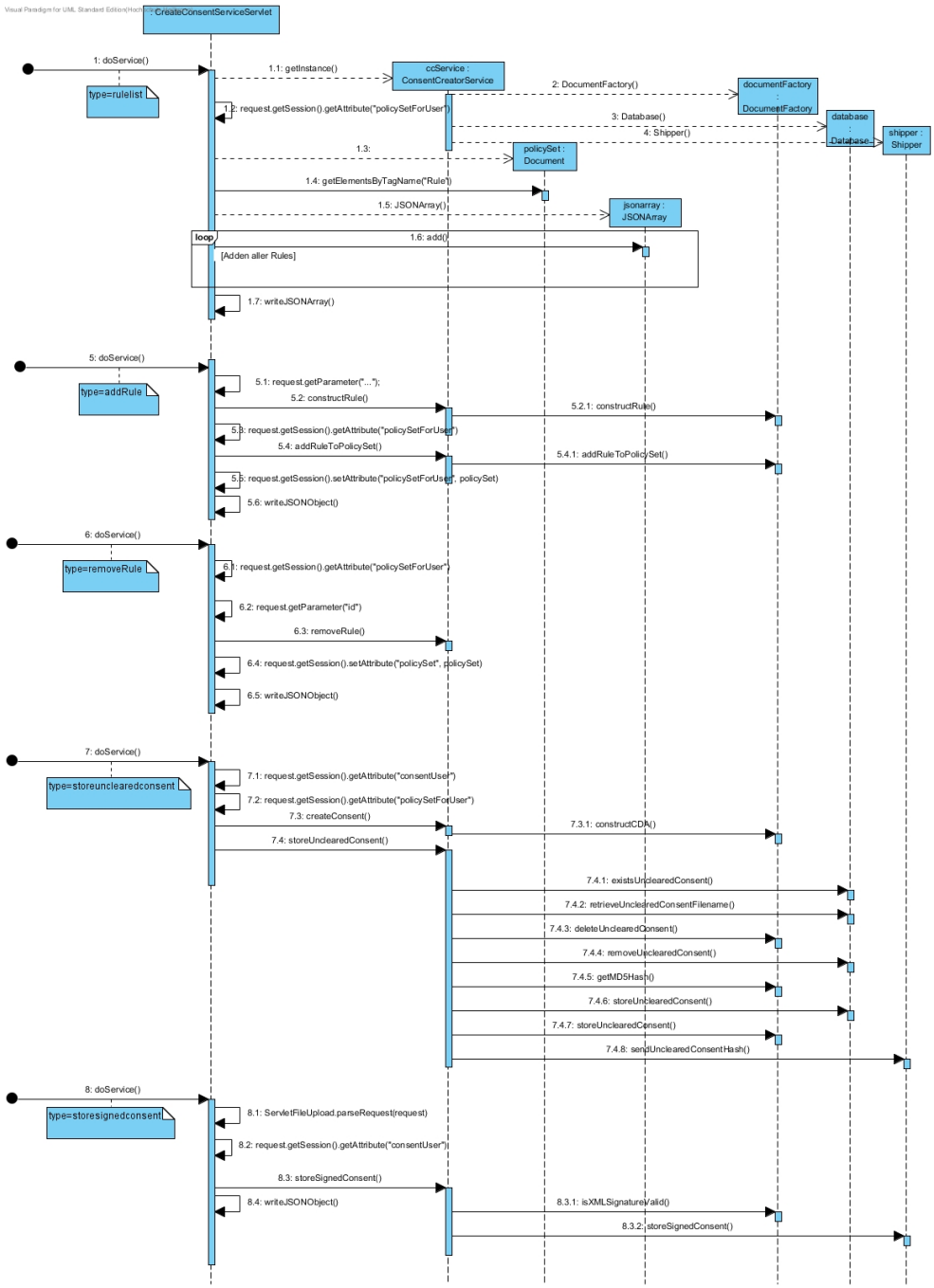

Abbildung 29: Sequenzdiagramm Use Case Einwilligungserklärung erstellen Leistungserbringer

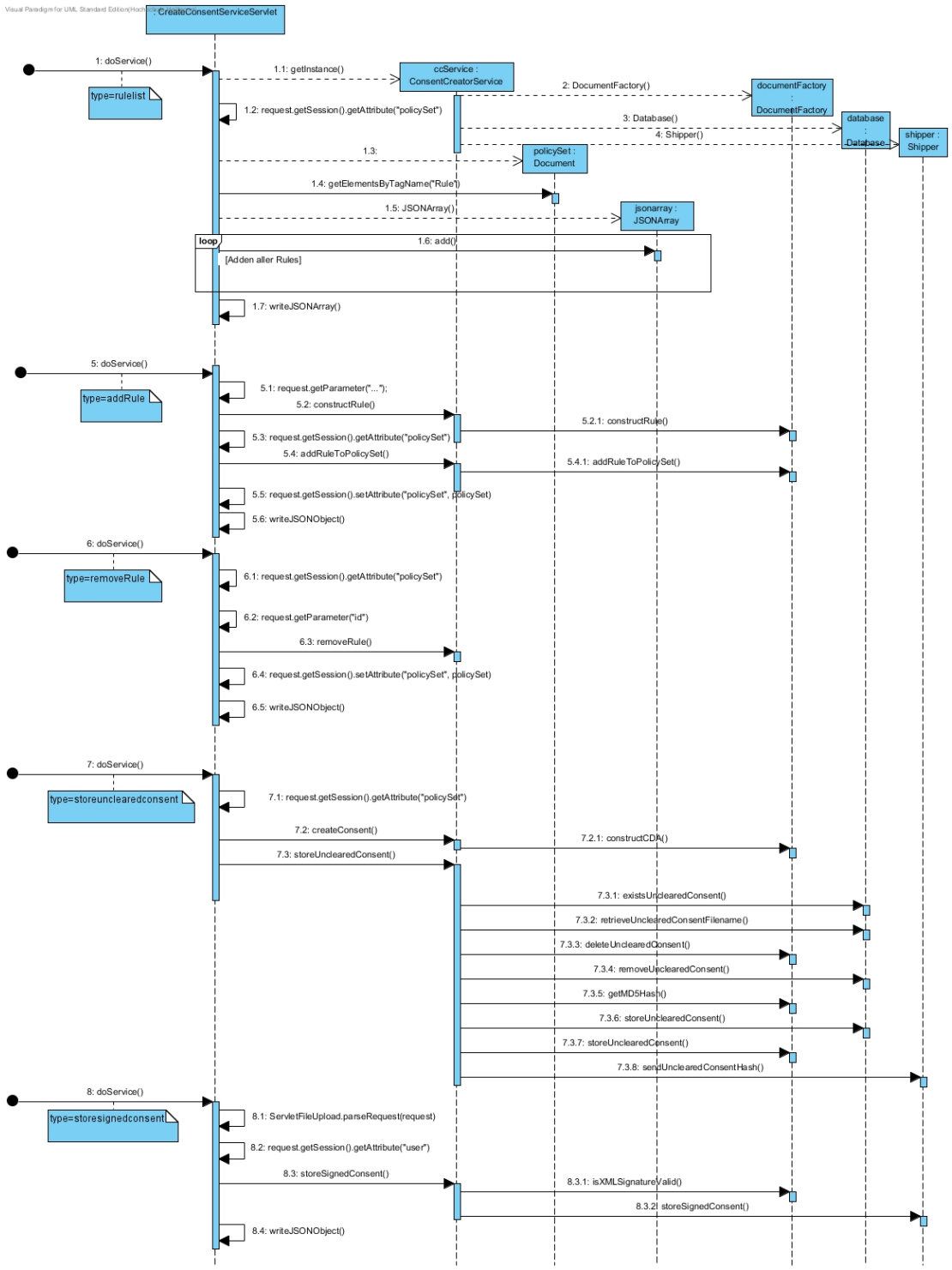

Abbildung 30: Sequenzdiagramm Use Case Einwilligungserklärung erstellen Patient

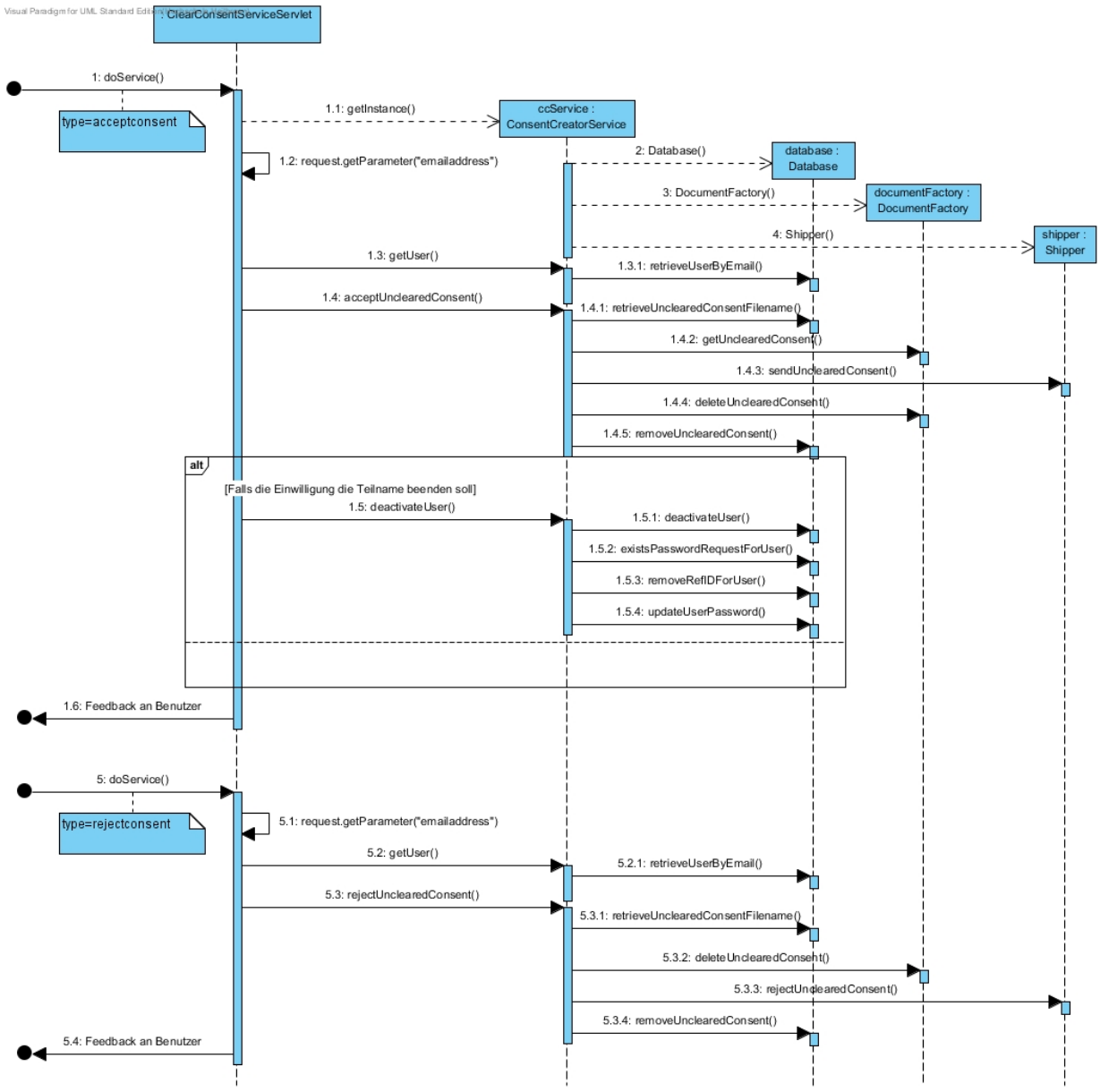

Abbildung 31: Sequenzdiagramm Use Case Einwilligungserklärung freischalten

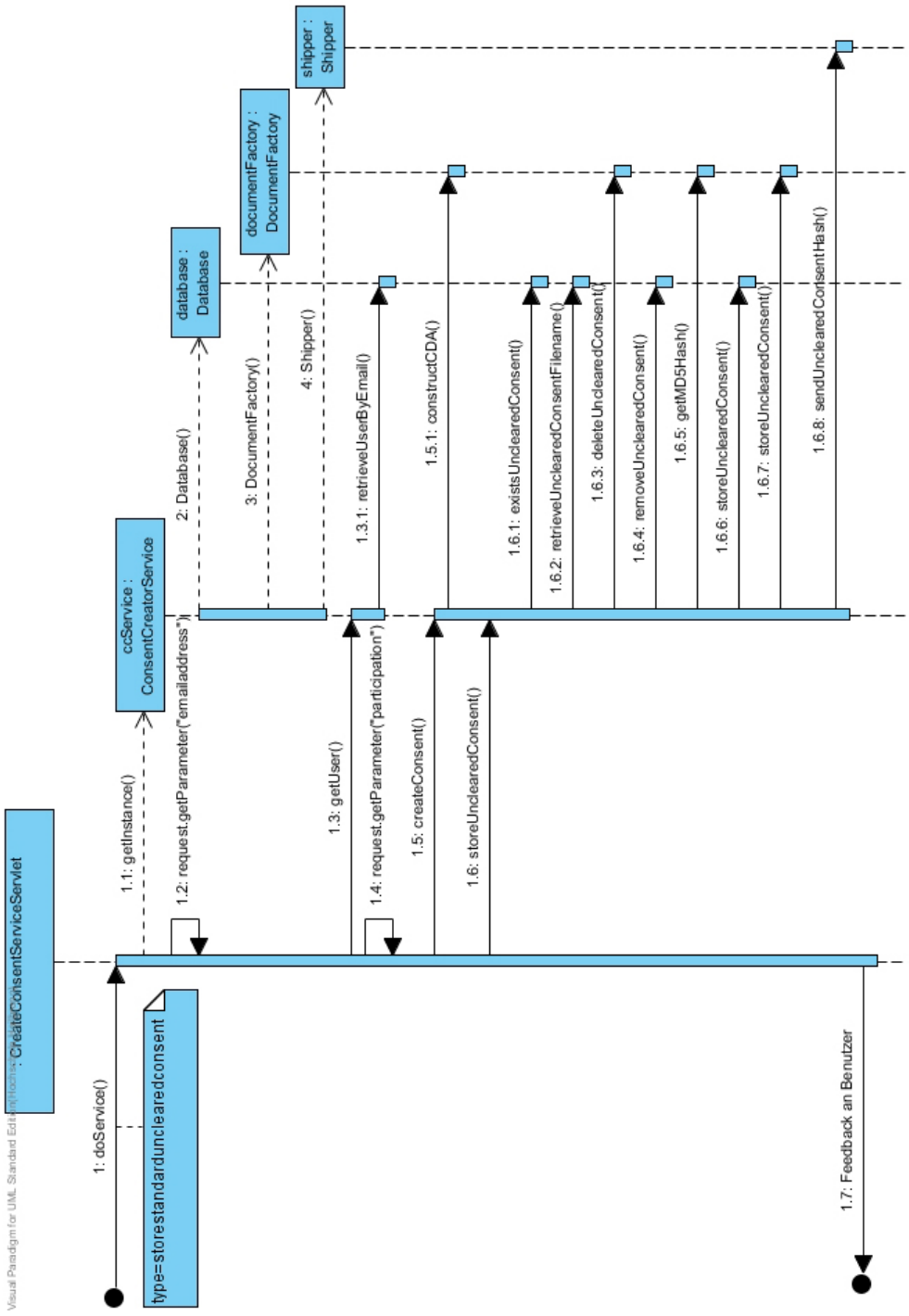

Abbildung 32: Sequenzdiagramm Use Case Einwilligungserklärung unsigniert speichern

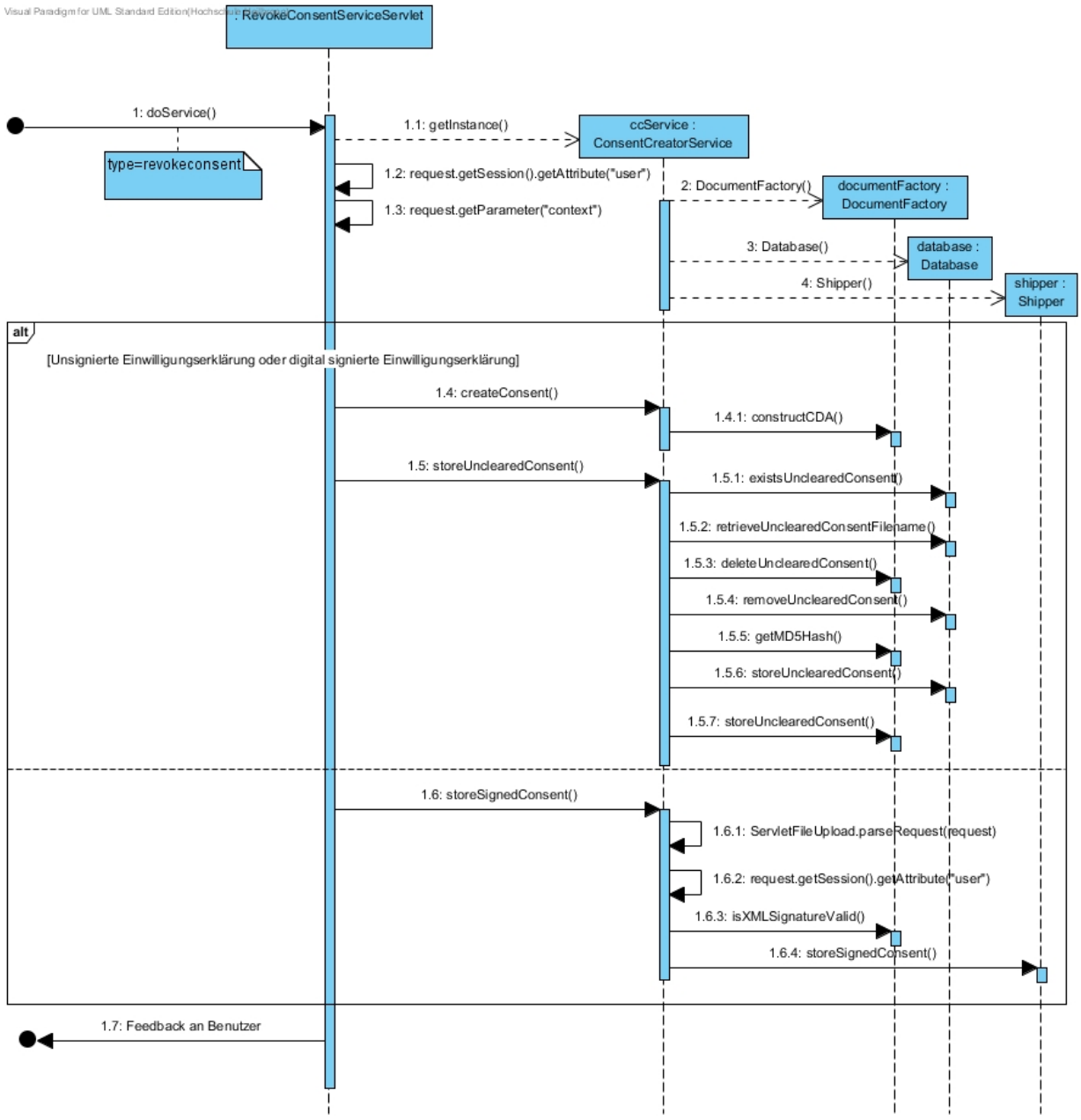

Abbildung 33: Sequenzdiagramm Use Case Einwilligungserklärung zurücksetzen

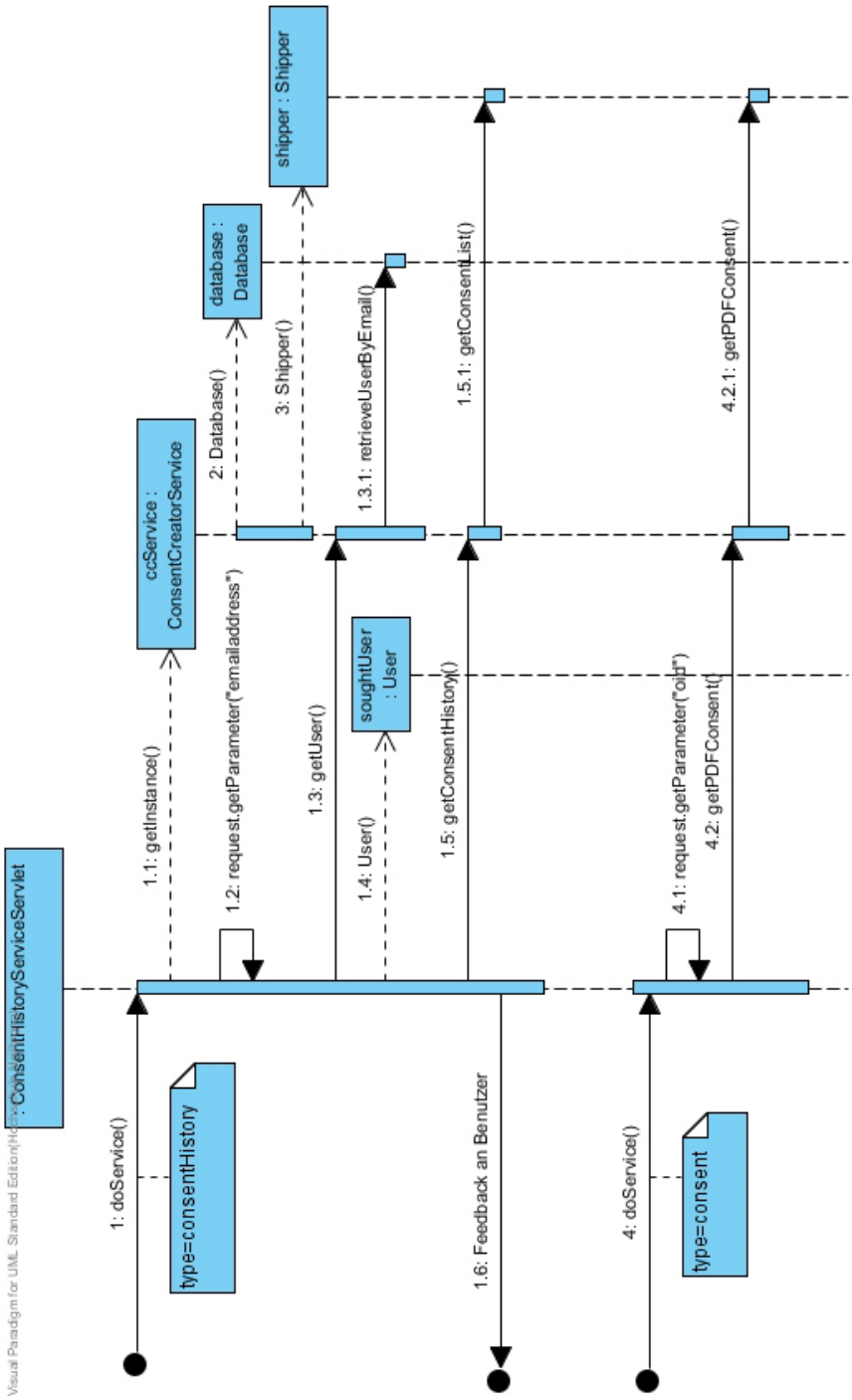

Abbildung 34: Sequenzdiagramm Use Case Einwilligungshistorie eines Patienten ansehen

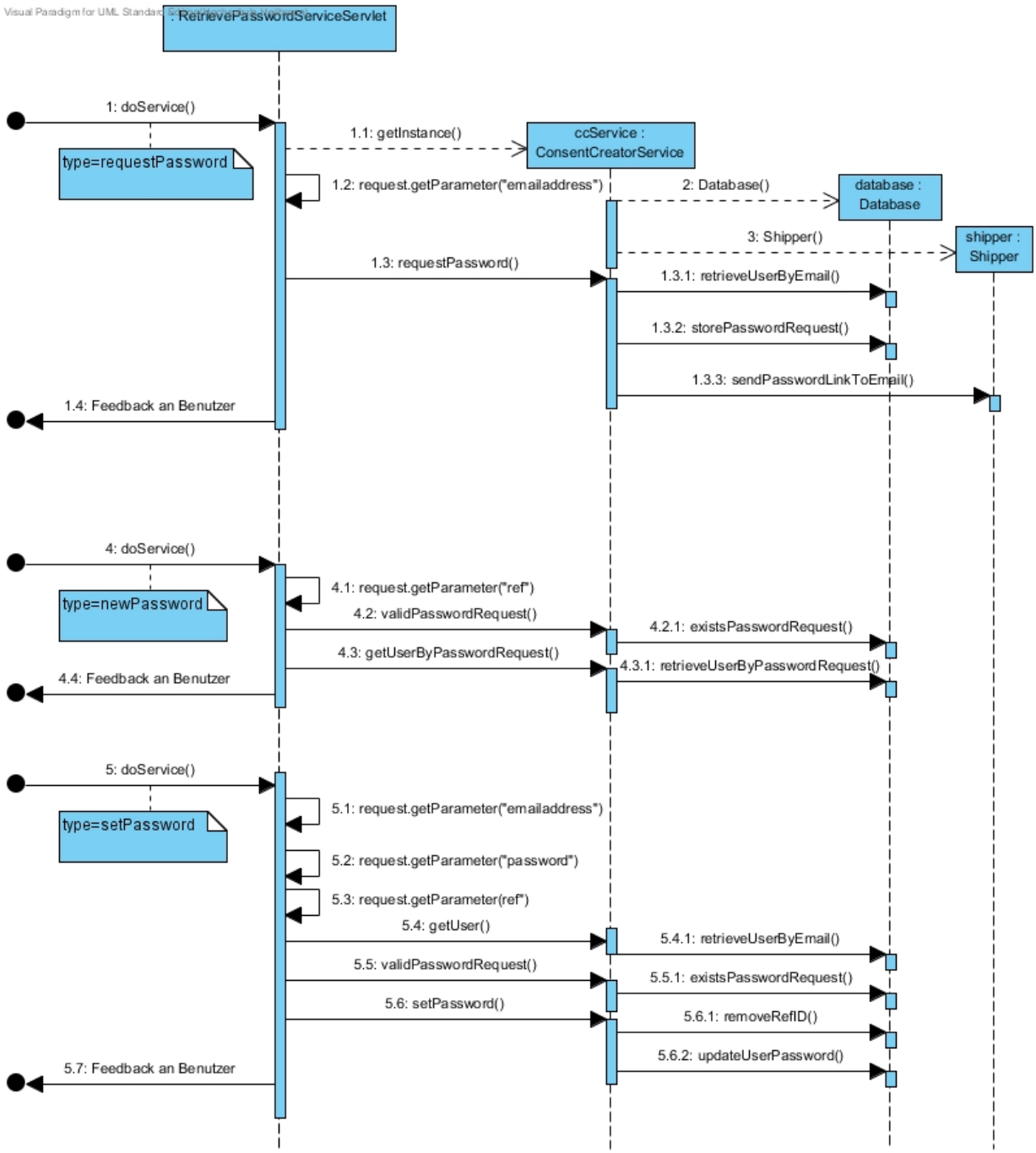

Abbildung 35: Sequenzdiagramm Use Case Passwort wiedererlangen

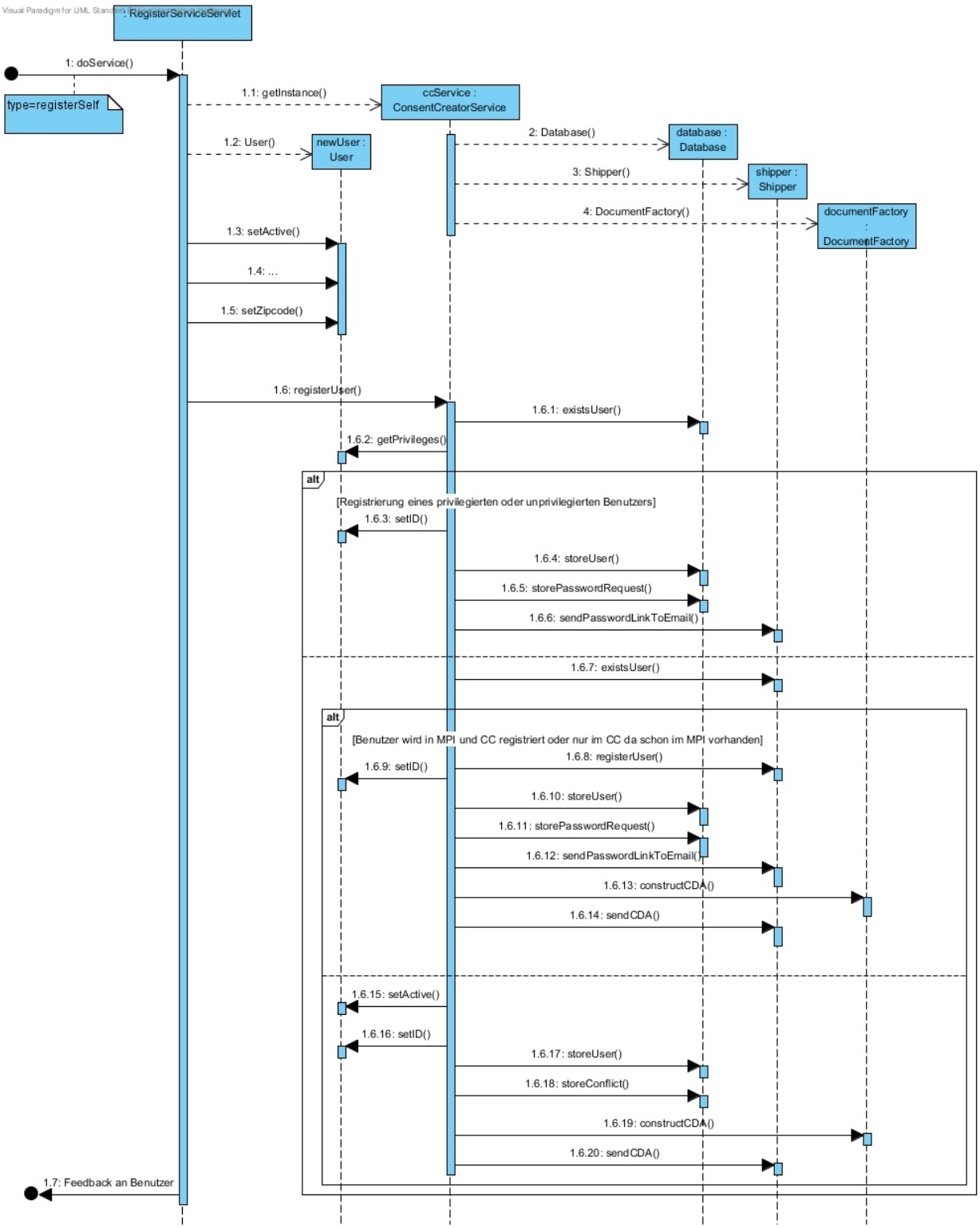

Abbildung 36: Sequenzdiagramm Use Case Registrieren

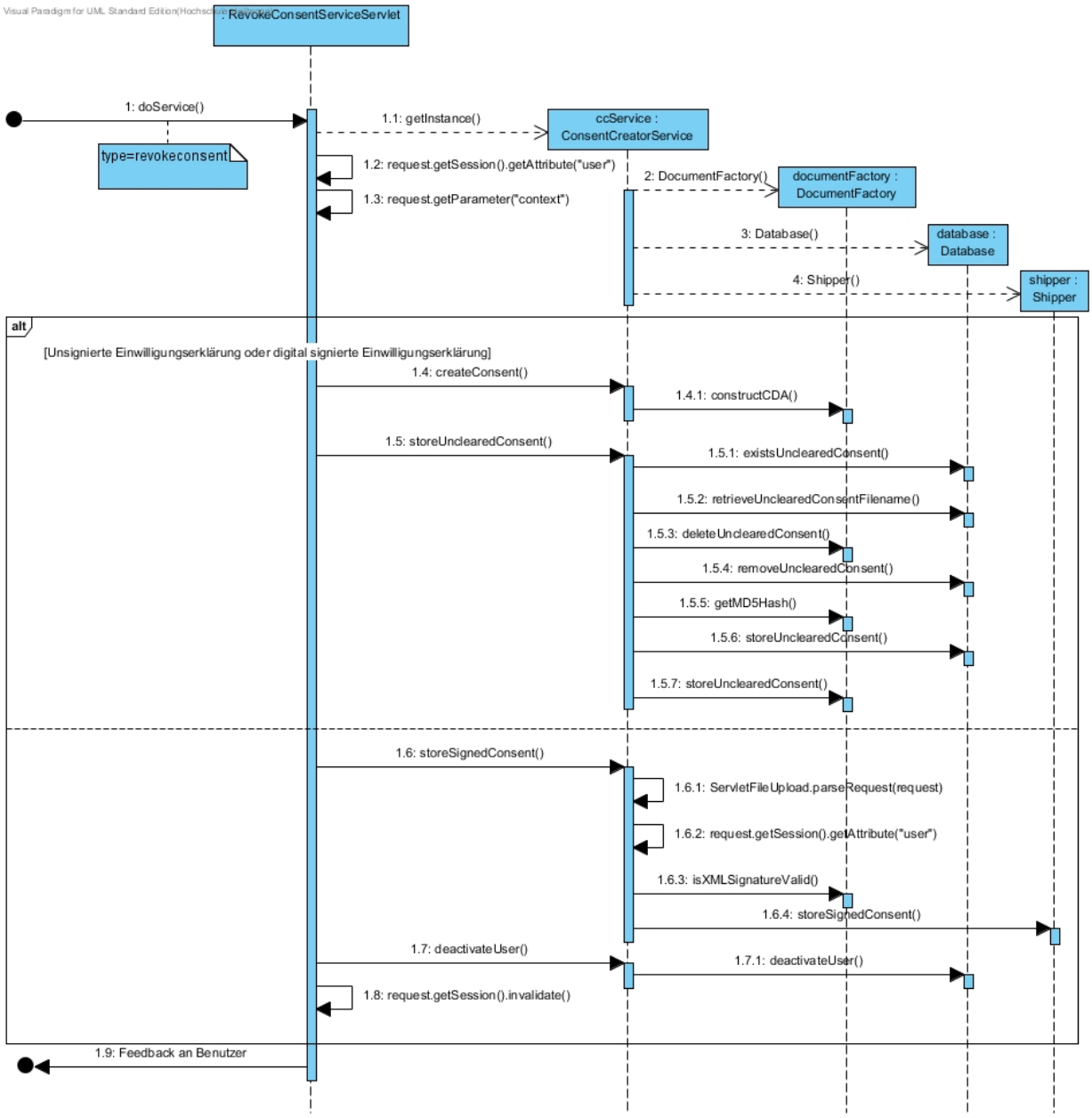

Abbildung 37: Sequenzdiagramm Use Case Teilnahme beenden

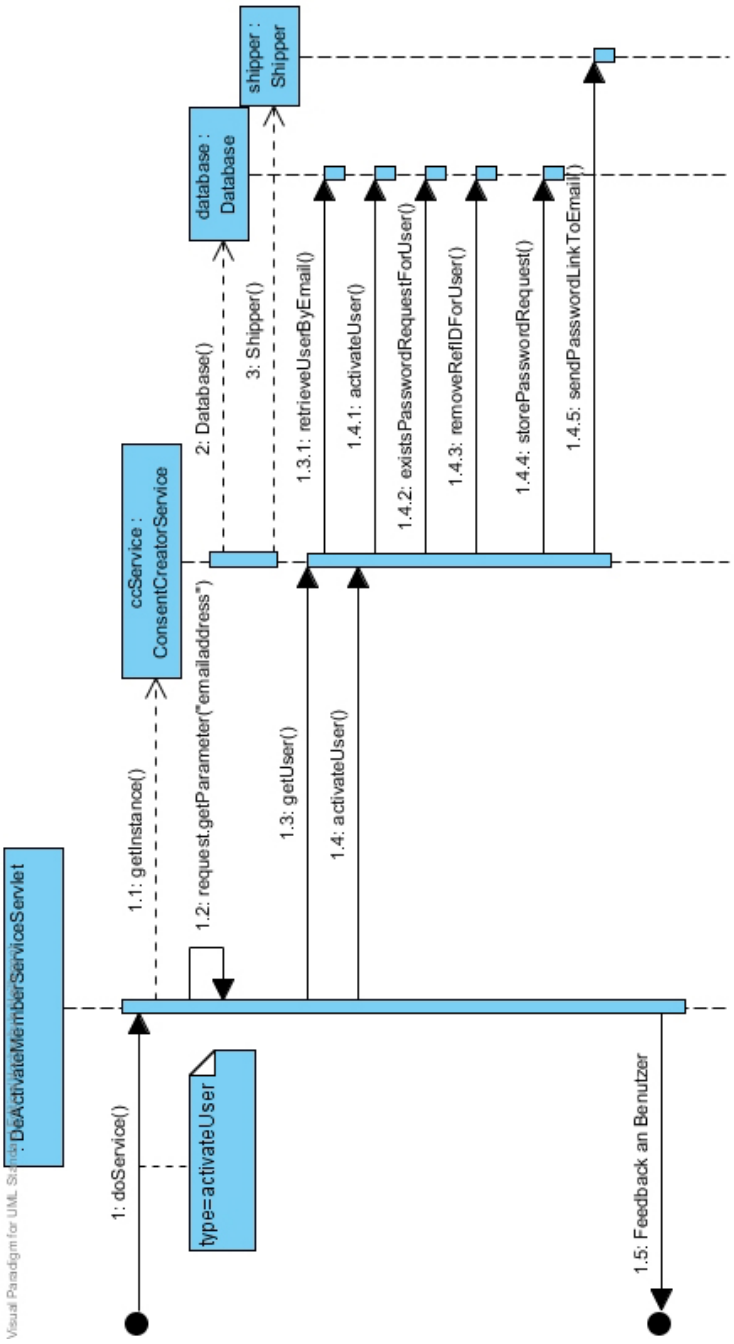

Abbildung 38: Sequenzdiagramm Use Case Teilnehmer aktivieren

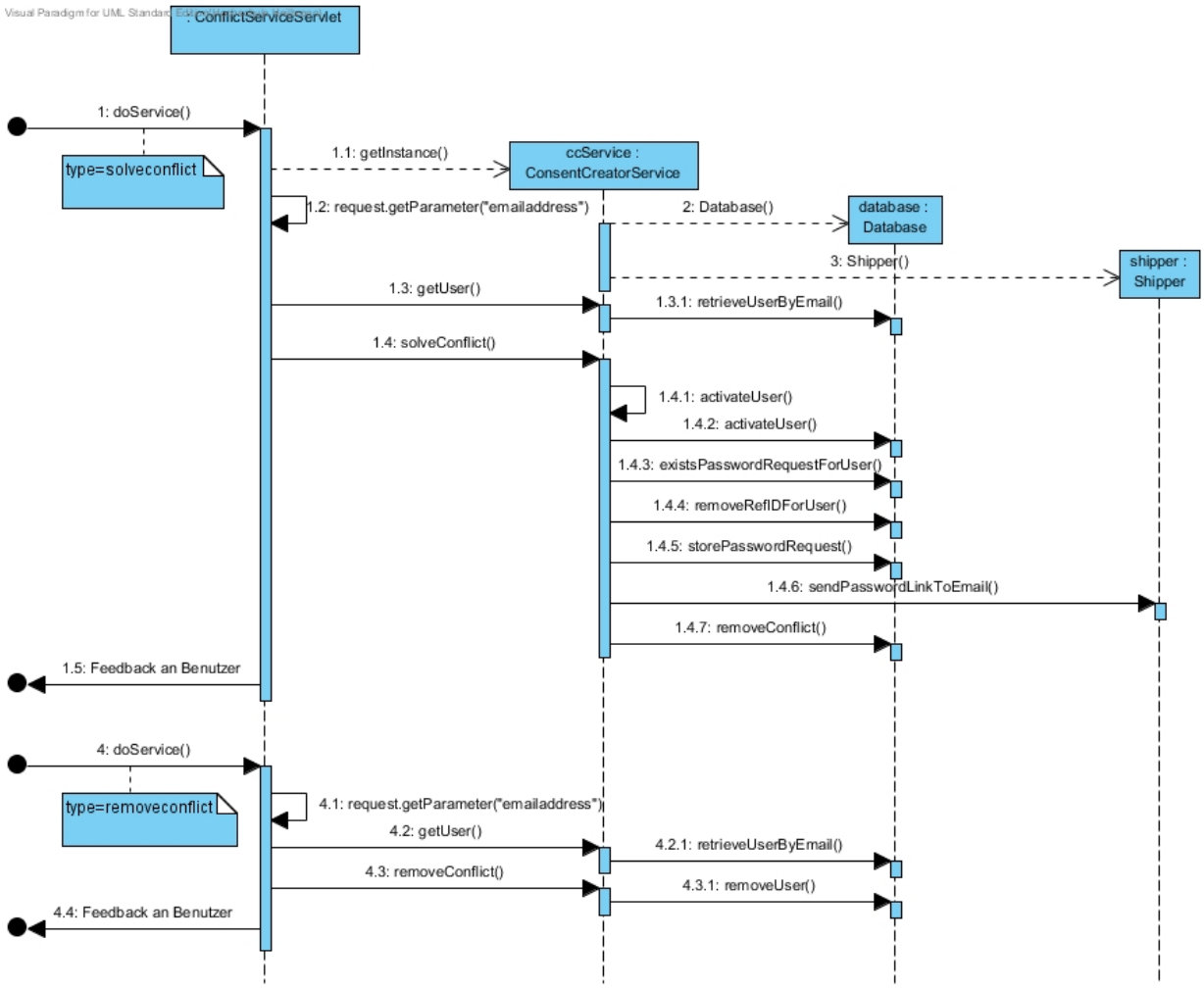

Abbildung 39: Sequenzdiagramm Use Case Teilnehmer freischalten

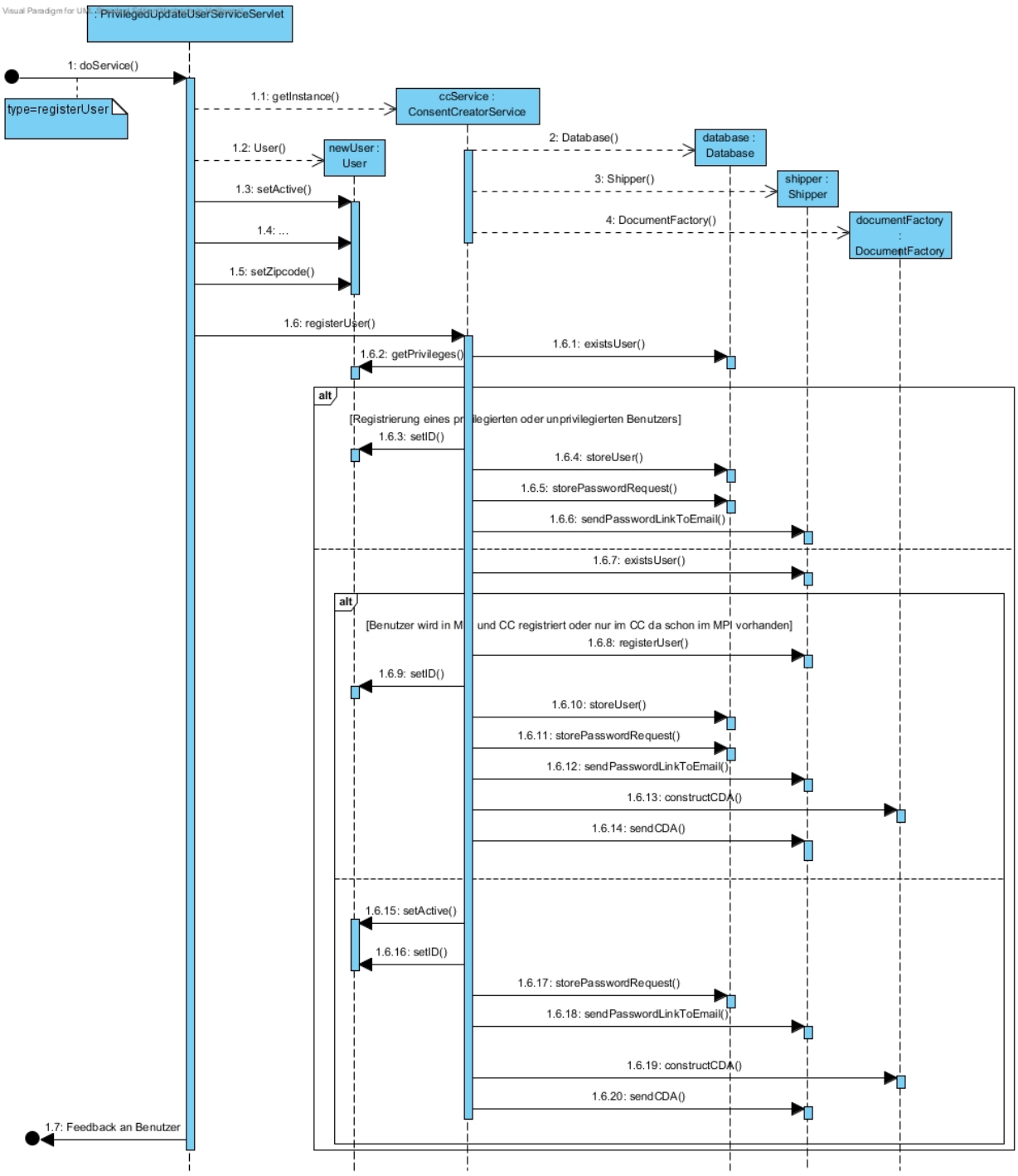

Abbildung 40: Sequenzdiagramm Use Case Teilnehmer hinzufügen

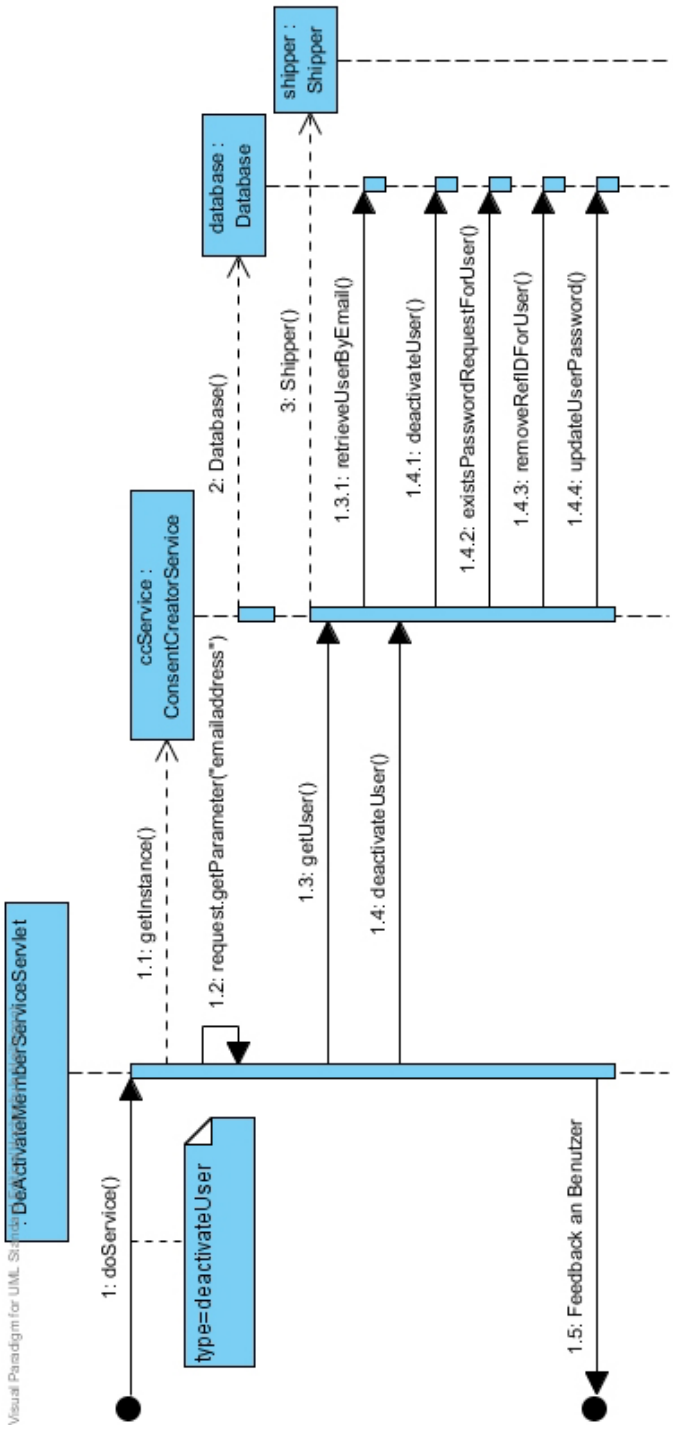

Abbildung 41: Sequenzdiagramm Use Case Teilnehmer inaktivieren

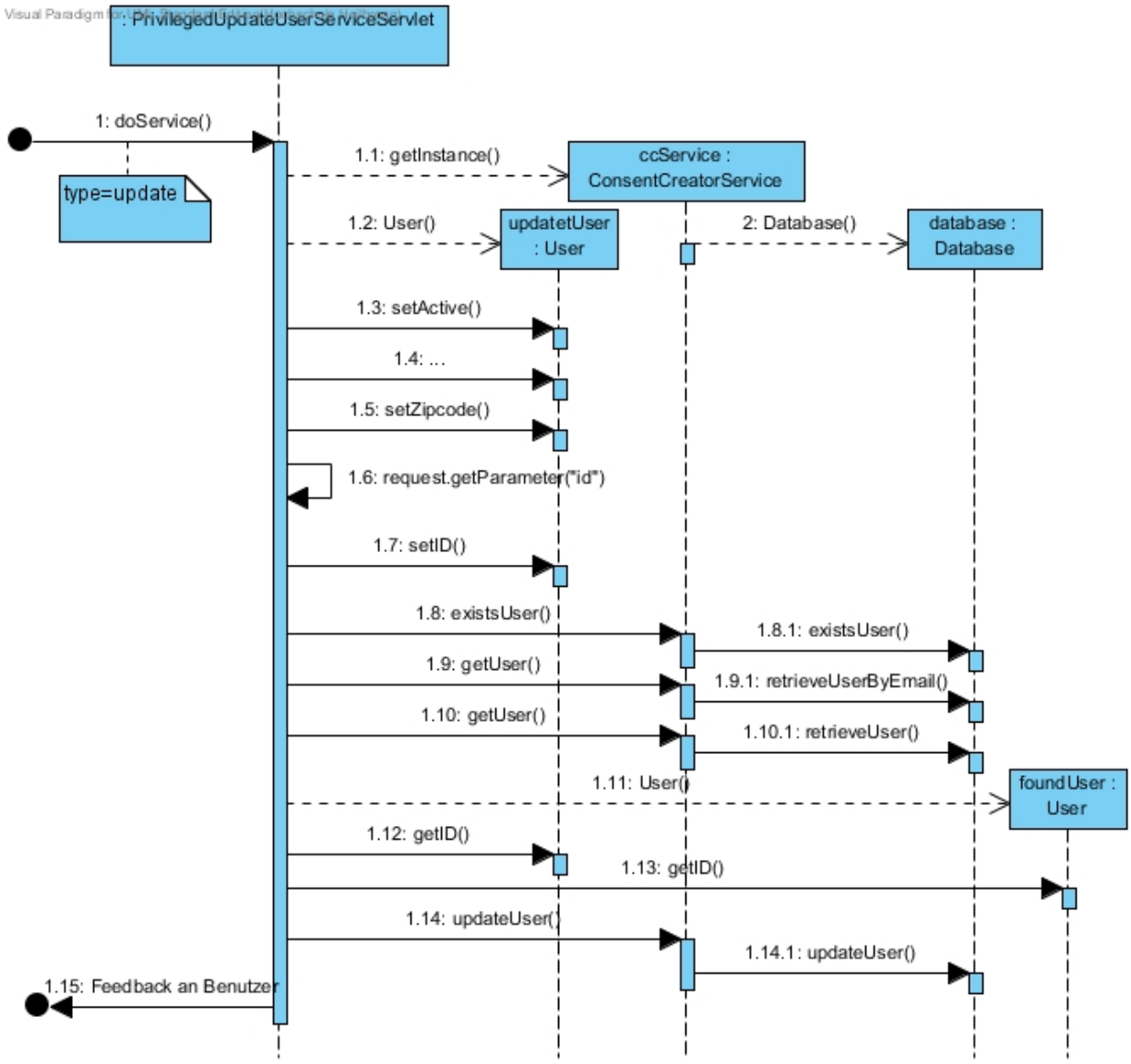

Abbildung 42: Sequenzdiagramm Use Case Teilnehmerdaten bearbeiten

B.4 Einwilligungserklärung

UniversitätsKlinikum Heidelberg

Einrichtungsübergreifende elektronische Patientenakte ISIS Einwilligungserklärung

Patient	Homo Heidelbergensis
Adresse	Sesamstraße 69120 Heidelberg
Geburtsdatum	31.01.2011
Aufklärende Stelle	123

Ich wurde über die Möglichkeit der Inanspruchnahme einer einrichtungsübergreifenden elektronischen Patientenakte im Rahmen des Intersektoralen Informationssystems (ISIS) ausführlich informiert. Ich erhielt eine schriftliche Patienteninformation und habe diese gelesen. Darüber hinaus wurde ich mündlich aufgeklärt und erhielt gestellte Fragen beantwortet.
Insbesondere wurde ich über Folgendes informiert:

1. Als ISIS-Teilnehmer wird für mich eine arztgeführte einrichtungsübergreifende elektronische Patientenakte angelegt. Hierin werden Daten und Dokumente zu meinen Behandlungen dauerhaft (bis zu Widerruf oder Ableben) gespeichert. Diese Speicherung erfolgt neben der offiziellen ärztlichen Dokumentation der mich behandelnden Ärzte in ihren Häusern.
2. Über die ISIS-Patientenakte können Ärzte und soweit erforderlich ihr Assistenzpersonal aus den mich behandelnden Fachabteilungen der von mir zugelassenen Krankenhäuser und Arztpraxen (Einrichtungen) auf meine verfügbaren Behandlungsdaten wie Diagnosen, Befunde, Berichte und administrative Daten zugreifen soweit dies für meine Versorgung erforderlich ist.
3. Der Zugriff auf meine Daten wird für Fachabteilungen der nachstehenden Einrichtungen gemäß der Formulierungen der jeweiligen Datenschutzregeln ermöglicht oder verwehrt. Mir ist bekannt, dass ich bei weiteren behandelnden Einrichtungen eine neue, erweiterte Erklärung abgeben kann und/oder diese Berechtigungen auch jederzeit einschränken kann.
   - Alle Chefärzte der Organisation Kreiskrankenhaus Schwetzingen dürfen alle meine, in ISIS verfügbaren, Arztbriefe lesen.
   - Alle Chefärzte der Organisation Universitätsklinikum Heidelberg dürfen alle meine, in ISIS verfügbaren, Laborberichte lesen.
   - Alle Oberärzte der Organisation Universitätsklinikum Heidelberg dürfen alle meine, in ISIS verfügbaren, Arztbrief lesen.
   - Alle Ärzte der Organisation Universitätsklinikum Heidelberg dürfen meine, in ISIS verfügbaren, Dokumente nicht lesen.

- Alle Ärzte der Organisation Kreiskrankenhaus Schwetzingen dürfen meine, in ISIS verfügbaren, Dokumente lesen.
- Die Organisation Kreiskrankenhaus Schwetzingen darf meine, in ISIS verfügbaren, Laborberichte nicht lesen.
- Die Organisation Kreiskrankenhaus Schwetzingen darf alle meine Dokumente in ISIS lesen.
- Die Organisation Universitätsklinikum Heidelberg darf keine meiner Dokumente in ISIS einstellen.
- Die Organisation UKHD darf alle meine Dokumente in ISIS lesen.
- Die Organisation Universitätsklinikum Heidelberg darf alle meine Dokumente in ISIS lesen.
- Grundsätzlich dürfen alle meine Daten, die in, an ISIS beteiligten, Organisationen erzeugt werden, in ISIS eingestellt werden.

4. Die ISIS-Patientenakte wird im Auftrag der teilnehmenden Krankenhäuser und Arztpraxen durch einen Betreiber verarbeitet (derzeit das Universitätsklinikum Heidelberg). Bei einem Betreiberwechsel erhalte ich rechtzeitig vorher Nachricht.
5. Ich kann mich zur Wahrnehmung meiner Rechte wie Auskunft, Einsicht, Sperrung, Widerruf an meinen behandelnden Arzt in einem der ISIS-Häuser oder die in der Aufklärung genannten Kontakte wenden. Im Falle eines Widerrufs werden meine bereits in der ISIS-Akte gespeicherten Daten gelöscht.

Erklärung:

Ich bin einverstanden, dass meine Daten in der dargestellten Weise verarbeitet und genutzt werden. Soweit dies für meine Versorgung und die Verwaltung der ISIS-Patientenakte erforderlich ist, **entbinde ich** meine behandelnden Ärzte und ihr Assistenzpersonal **von ihrer Schweigepflicht**.
Diese Erklärung erfolgt **freiwillig** und kann jederzeit **widerrufen** werden. Eine Nichterteilung der Einwilligung oder ein Widerruf hat - bis auf den Verzicht der Vorteile von ISIS - keine nachteilige Wirkung auf meine Behandlung. Ich bin informiert, dass ich stattdessen auch vorübergehend alle Zugriffsrechte sperren lassen kann.
Eine Mehrfertigung dieser Erklärung habe ich erhalten.

Heidelberg, den	
Unterschrift Patient	Unterschrift Aufklärender
Ggf. Unterschrift gesetzl. Vertreter	

Verwaltungsvermerk:

Obiger Patient wurde aufgeklärt nach den Richtlinien der Kurzaufklärung Version 1.0	Ja ❑ Nein ❑
Das Einwilligungskennzeichen im KIS wurde entsprechend der Einwilligung gesetzt	Ja ❑ Nein ❑
Datum/Kürzel Aufklärender	

C Literaturverzeichnis

[Ärzteblatt 2007] Parzeller, Markus; Wenk, Maren; Zedler, Barbara; Rothschild, Markus; *Aufklärung und Einwilligung bei ärztlichen Eingriffen*; Dtsch Arztebl 2007; 104(9): A-576 / B-507 / C-488

[Birkle 2009a] Birkle M., Heinze O., Bergh B. *Entwurf eines elektronischen Einwilligungsmanagements für ein Intersektorales Informationssystem.* Tagungsband der eHealth2010. 6.-7.Mai 2010; Wien. OCG; 2010.

[Birkle 2009b] Birkle M. *Konzept für das Einwilligungsmanagement in einem intersektoralen Informationssystem* Diplomarbeit, Universität Heidelberg/Hochschule Heilbronn

[Brenner 2001] Brenner G. *Spezielle Anwendungen in der Gesundheitstelematik.* Z. ärztl. Fortbild. Qual.sich., 2001;95: 646-651.

[BSI 2006] Bundesamt für Sicherheit in der Informationstechnik - *Grundlagen der elektronischen Signatur* - 2006

[BSI 2010] BSI: Elektronische Signatur - *https://www.bsi.bund.de/ContentBSI/Publikationen/Faltblaetter/F10ElektronischeSignatur.html* Version: 2010, Abruf: 10.08.2010

[Bund 2001] Bund: Signaturverordnung (SigV) Bundesrepublik Deutschland *http://www.gesetze-im-internet.de/sigv_2001/* Version: 2001 Abruf: 05.02.2011

[Bund 2009a] Bund: Bundesdatenschutzgesetz (BDSG) Bundesrepublik Deutschland *http://www.gesetze-im-internet.de/bdsg_1990/* Version: 2009 Abruf: 05.02.2011

[Bund 2009b] Bund: Signaturgesetz (SigG) Bundesrepublik Deutschland *http://www.gesetze-im-internet.de/sigg_2001/* Version: 2009 Abruf: 05.02.2011

[Bund 2010a] Bund: Strafgesetzbuch (StGB) Bundesrepublik Deutschland *http://www.gesetze-im-internet.de/stgb* Version: 2010 Abruf: 05.02.2011

[Bund 2010b] Bund: Bürgerliches Gesetzbuch (BGB) Bundesrepublik Deutschland *http://www.gesetze-im-internet.de/bgb/* Version: 2010 Abruf: 05.02.2011

[Bund 2010c] Bund: Zivilprozessordnung (ZPO) Bundesrepublik Deutschland *http://www.gesetze-im-internet.de/zpo/* Version: 2010 Abruf: 05.02.2011

[Caumanns 2008] Caumanns J.: *Übergreifendes Sicherheitskonzept für Umsetzung und Betrieb elektronischer Fallakten* 2008.

[COPRAS 2007] Cooperation Platform for Research & Standards - *Standardization Guidelines for IST research projects interfacing with ICT standards organizations* - 2007

[De-Mail 2010] Bundesministerium des Inneren, IT-Stab, Referat IT 1 - Informationsbroschüre *So einfach wie E-Mail, so sicher wie Papierpost.*

[DIG 2001] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone *Handbook of applied cryptography* Fifth Printing (August 2001) ISBN: 0-8493-8523-7

[DIG 2008] Hackel, S.; Roßnagel, A.: *Langfristige Aufbewahrung elektronischer Dokumente.* In: Klumpp, D.; Kubicek, H.; Roßnagel, A.; Schulz, W. (Hrsg): Informationelles Vertrauen für die Informationsgesellschaft. Berlin, Heidelberg: Springer 2008, 199-207.

[DIG 2010] C. Seidel, H. Kosock, A. Brandner, J. Balfanz, P. Schmücker *Empfehlungen für den Einsatz elektronischer Signaturen und Zeitstempel in Versorgungseinrichtungen des Gesundheitswesens* - CCESigG

[Heinze et al. 2008a] Heinze O., Brandner A., Brandner R., Bergh B. *Aufbau einer einrichtungsübergreifenden Patientenakte in der Rhein-Neckar-Region.* Telemed; 2008b 04.06.2008; Berlin; Schug, S. Engelmann, U. (Hrsg.); 2008b. p. 152-6.

[Heinze et al. 2008b] Heinze O., Bergh B. *Establishing a Personal Electronic Health Record (PEHR) in the Rhine-Neckar Region.* Informatica Medica Slovenica 2008; 13(2)

[Heinze et al. 2008c] Heinze O., Brandner A., Brandner R., Bergh B. *Auf dem Weg zur Persönlichen Einrichtungsübergreifenden Elektronischen Patientenakte.* EHEALTHCOM. 2008a:57-9.

[Heinze et al. 2010] Heinze O., Ihls A., Bergh B. *Development of an Open Source Provider and Organization Registry Service for Regional Health Networks*

[HL7 2005] ANSI/HL7 CDA, R2-2005 HL7 Clinical Document Architecture, Release 2 21.04.2005

[HL7 2006] HL7 Reference Information Model - Version: V 02-14 (13.07.2006) - ModelID: RIM_0214

[HL7 2007] *Getting Started with HL7 v3 and BizTalk Server 2006* by Elizabeth Redding http://msdn.microsoft.com/en-us/library/bb967001(BTS.10).aspx. Version: 2010, Abruf: 12.07.2010

[HL7 2010a] Health Level 7 International. *http://www.hl7.org/* Version: 2010, Abruf 12.07.2010

[HL7 2010b] HL7 Benutzergruppe in Deutschland e.V. *http://www.hl7.de/* Version: 2010, Abruf 12.07.2010

[ICW 2009a] ICW: Prdouktbroschüre - Professional Exchange Server (PXS) - Oktober 2009

[ICW 2009b] ICW: Produktwebseite ICW Professional Exchange Server (PXS). *http://www.icw-global.com/de/de/loesungen-produkte/icw-professional-suite/fuer-kliniken/professional-exchange-server.html* Abruf: 15.07.2010

[IHE 2009a] IHE IT Infrastructure (ITI)) Technical Framework Volume 1 (ITI TF-1) - Integration Profiles - Revision 6.0 - Final Text - August 10, 2009

[IHE 2009b] IHE Patient Care Coordination (PCC) Technical Framework Volume I - Revision 5.0 - Final Text - August 10, 2009

[IHE 2010a] Integrating the Healthcare Enterprise (IHE) International, Incorporated Principles of Governance - March 4, 2010

[IHE 2010b] IHE.net - Integrating the Healthcare Enterprise. *http://www.ihe.net/*. Version: 2010, Abruf 20.07.2010

[IHE 2010c] IHE.net - Connectathon Overview. *http://www.ihe.net/Connectathon/*. Version: 2010, Abruf 20.07.2010

[ISO 2004] ISO/IEC Guide 2:2004

[ISO 2010] ISO: International Organisaton for Standardization (ISO). *http://www.iso.org* Version: 2010, Abruf 22.06.2010

[Land 2007] Land Baden-Württemberg: Landeskrankenhausgesetz Baden-Württemberg (LKHG BW) *http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=KHG+BW&psml=bsbawueprod.psml&max=true&aiz=true* Abruf: 05.02.2011

[Meier 2003] Meier, A., *Der rechtliche Schutz patientenbezogener Gesundheitsdaten*, in: Münsteraner Reihe 84, Verlag für Versicherungswirtschaft, Karlsruhe 2003

[Namli und Dogac 2006] Namli T., Dogac A.: *Implementation Experiences on IHE XUA and BPPC.* Ankara, Turkey: Middle East Technical University 2006.

[OASIS 2010] OASIS: Website Organization for the Advancement of Structured Information Standards (OASIS). *http://www.oasis-open.org/.* Version: 2010, Abruf: 29.06.2010

[PDFA 2010] PDF/A An ISO Standard. *http://www.pdfa.org/* Version: 2010, Abruf: 29.06.2010

[PKCS 2004] PKCS #11 v2.20: Cryptographic Token Interface Standard

[Schmücker et al. 1998] Schmücker P et al.: *Die elektronische Patientenakte- Ziele, Strukturen, Präsentation und Integration.* Informatik, Biometrie und Epidemiologie in Medizin und Biologie, 29(3-4), 1998;221-241

[Schneider 2010] Schneider, B., O. Heinze, et al. (2010). Development of a Teleradiology web portal for the exchange of medical data using DICOM e-mail. 13th World Congress on Medical and Health Informatics, Capetown, South Africa.

[Tuffs 2007] Tuffs A. BMJ : British Medical Journal *German ethics council demands opt-out system for transplants* BMJ. 2007 May 12; 334(7601): 973.

[Warda 2005] Warda F: *Elektronische Gesundheitsakten.* Rheinware Verlag, Mönchengladbach: 2005

[XACML 2005] eXtensible Access Control Markup Language (XACML) Version 2.0

[XML 2004] *XML in a Nutshell, 3rd edition* by Elliotte Rusty Harold & W. Scott Means. O'Reilly 2004

[XML 2008] Extensible Markup Language (XML) 1.0 (Fifth Edition) - W3C Recommendation 26 November 2008

[XSLT 2007] XSL Transformations (XSLT) Version 2.0 - W3C Recommendation 23 January 2007

[XSLT 2008] *A Critical Analysis of XSLT Technology for XML Transformation* - Gregory Sherman, Senior Technical Report April 2008

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; die aus fremden Quellen (einschließlich elektronischer Quellen) direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Datum Lennart Köster